BANCA
SISTEMA

BANCA SISTEMA S.p.A.

Organisation and Management Model

pursuant to article 6, paragraph 1, letter a),
of Legislative Decree No. 231
of 8 June 2001, as amended

May 2018 Version

TABLE OF CONTENTS

- GENERAL PART
- 1.Law and regulatory framework 4

1.1 Introduction 4
1.2 The predicate offences 6
1.3 The applicable sanctions 7
1.4 Exemption from administrative liability 9

- 2.Adoption of the Model 11

2.1 Aims pursued by adopting the Model 11
2.2 Corporate governance model 13
2.3 The proxy and power of attorney system 15

- 3.Purpose of the Model 17

3.1 The Model of Banca Sistema 17
3.2 The Model's preliminary activity 18
3.3 Approval of the Model and its implementation 20

- 4.The Supervisory Body 21

4.1 Requirements 21
4.2 Procedure to convene and to hold the meetings of the SB 23
4.3 Duties and powers of the SB 24
4.4 Information flows towards the Supervisory Body 26
4.5 Information flows from the Supervisory Body towards the corporate bodies 29
4.6 Rules of operation of the SB 29

- 5.Communication plan 30

5.1 Introduction 30
5.2 Spreading and training 31

- 6.Disciplinary system 33

6.1 General principles 33
6.2 Measures against the Directors 34
6.3 Measures against the members of the Board of Statutory Auditors 35
6.4 Sanctioning system against the executives 35
6.5 Sanctioning system against the employees 35
6.6 Measures against external collaborators 38

- SPECIAL PART 40
- Purpose of the Special Part 41
- A) CRIMES AGAINST THE PUBLIC ADMINISTRATION 43
- 1 Crimes against the Public Administration 45
- 2 Areas at risk of crime 53
- 3 Rules of Conduct 54
- 4 The Supervisory Body's duties 59
- B) CORPORATE CRIMES 60
- 1 Corporate crimes 60
- 2 Areas at risk from the commission of offences 68
- 3 Rules of Conduct 69
- 4 The Supervisory Body's duties 73
- C) MARKET ABUSE 74
- 1 Market abuse 74
- 2 Areas at risk of crime 77
- 3 Rules of conduct 79
- 4 The Supervisory Body's duties 80
- D) MONEY LAUNDERING CRIMES 82
- 1 Receiving, laundering or using money, goods or benefits of illicit origin, and self-laundering 82
- 2 Areas at risk from the commission of offences 85

- 3 Rules of Conduct 86
- 4 The Supervisory Body's duties....89
- E) COMPUTER CRIMES AND UNLAWFUL PROCESSING OF DATA....91
- 1 Computer crimes and unlawful processing of data....91
- 2 Areas at risk of crime....102
- 3 Rules of Conduct 102
- 4 The Supervisory Body's duties....106
- F) OCCUPATIONAL HEALTH AND SAFETY OFFENCES 108
- 1 Occupational health and safety offences....108
- 2 Areas at risk of crime....109
- 3 Rules of Conduct 110
- 4 The Supervisory Body's Duties....118

1. Law and regulatory framework

1.1 Introduction

Legislative Decree No. 231 of 8 June 2001 (hereinafter, "Legislative Decree No. 231/2001" or the "Decree"), containing the "Provisions on the administrative liability of legal entities, companies and associations, even if lacking legal personality (hereinafter, the "Entity" or "Entities"), pursuant to article 11 of Law No. 300 of 29 September 2000", has introduced in Italy, for the very first time, an administrative liability arising out of crime weighing on legal entities (or "Entities"), which is added to that of the natural person having physically committed the wrongful act.

It is the case of a new and broader form of liability, which affects the Entity for some crimes committed - or even only attempted - in its interest or to its advantage, by persons who are functionally bound thereto (top management and persons under the latter's management and supervision).

The Decree foresees that the Entities may be held liable and, thus, sanctioned, exclusively in connection with the perpetration of some crimes (the so-called "predicate offences") peremptorily mentioned by law, regardless of the fact that the list may be amended and completed by the legislator.

It is the Decree's intention to align the domestic laws and regulations on the liability of legal entities with some international conventions to which Italy had already adhered for quite some time[1].

The first main indictment criterion thus consists in the fact that the crime was committed in the interest or to the advantage of the Entity: this means that the Entity shall be liable if the wrongful act was committed to favour the Entity, without it being necessary to effectively and specifically achieve the aim.

[1] Such as the Brussels Convention of 26 July 1995 on the protection of the European Communities' financial interests, the Convention of 26 May 1997, also signed in Brussels, on the fight against corruption, and the OECD Convention of 17 December 1997 on combating bribery of foreign public officials in international business transactions.

The Entity shall not be liable if the offence was committed by one of the persons mentioned above exclusively in its own interest or in the interest of third parties.

The second main indictment criterion consists in the type of persons perpetrating the crime, who may bring about the Entity's administrative liability.

Precisely, the aforesaid persons may be:

- top management (such as, for instance, the legal representative, the directors, the general manager, or the persons managing or controlling the Entity, even *de facto*);
- subordinate staff, normally employees, but also persons from outside the Entity, who have been entrusted with a mandate to be fulfilled under the management and supervision of top management.

Should different persons contribute to committing the crime (section 110 of the Criminal Code), it shall not be necessary for the so-called 'qualified' person to directly carry out the wrongful act, but it shall be sufficient for the latter to provide an acquainted causal contribution to the perpetration of any such crime.

The liability foreseen under the aforesaid Decree shall also arise in respect of the crimes committed by the Entity abroad, under the following conditions:

- the crime was committed by a person functionally bound to the Entity (either top management or subordinate staff, as explained above);
- the Entity's principal place of business is located in Italy;
- the Entity may solely be liable in the cases and under the conditions provided for under sections 7, 8, 9 and 10 of the Criminal Code and, should the law foresee that the guilty natural person be punished upon the request of the Ministry of Justice, the Entity shall solely be prosecuted if the request is also raised against the Entity itself;
- the Entity shall solely be liable if the State of the place in which the crime was committed does not prosecute the aforesaid Entity.

The Entity's administrative liability shall also arise in the event that one of the offences foreseen under the Decree is committed even only as an attempt (section 56 of the Criminal Code).

1.2 The predicate offences

The crimes leading to the application of the administrative liability regime weighing on the Entities, for which the rules at issue apply, have been gradually extended compared to those at the time of its promulgation and, to date, include the crimes listed below:

a) **crimes committed in dealing with the Public Administration** (articles 24 and 25);
b) **computer crime and unlawful data processing** (article 24-*bis*);
c) **organised crime offences** (article 24-*ter*);
d) **crimes related to the forgery of money (coins and paper money), public credit currency, revenue stamps, and identification instruments or marks** (article 25-*bis*);
e) **crimes against industry and trade** (article 25-*bis*.1);
f) **corporate crimes** (article 25-*ter*);
g) **crimes aimed at terrorism or at subverting democratic order** (article 25-*quater*);
h) **female genital mutilation practices** (article 25-*quater*.1);
i) **crimes against individual personality** (article 25-*quinquies*);
l) **market abuse crimes** (article 25-*sexies*)
m) **transnational crimes** (Law No. 146/2006);
n) **manslaughter crimes and serious or very serious injury committed by breaching the laws and regulations on the protection of health and safety in the workplace** (article 25-*septies*);
o) **crimes of receiving stolen goods, money laundering and utilisation of money, goods or benefits of unlawful origin** (article 25-*octies*);
p) **copyright infringement crimes** (article 25-*novies*);
q) **crime of inducement not to make declarations or to make mendacious declarations to the judiciary** (article 25-*decies*);
r) **environmental crimes** (article 25-*undecies*);
s) **employment of illegally staying third-country nationals** (article 25-*duodecies*).

The crimes and the administrative offences cross-referenced above may lead to the administrative liability of the Entity having its principal place of business within the Italian territory, even if committed abroad.

As specified below in detail, in the Special Part of this document, we will only deal with the predicate offences which the Bank may assume in abstract terms.

1.3 The applicable sanctions

The sanctions weighing upon the Entity foreseen under Legislative Decree No. 231/2001, as a result of the commission or attempted commission of the predicate offences, are the following:

- Pecuniary sanction: applicable to all offences, fixed by the criminal Judge through a system based on "units" for a number of not less than one hundred and not in excess of one thousand, each for a value between a minimum of Euro 258.23 and a maximum of Euro 1,549.37[2]. The Judge shall fix the number of units by taking into consideration the seriousness of the wrongful act, the level of liability of the Entity, as well as the activity carried out to remove or mitigate the consequences of the wrongful act, and to prevent the commission of further offences. The amount of the unit is fixed based on the Entity's financial and asset conditions, for the purpose of ensuring the effectiveness of the sanction.

  The pecuniary sanction shall be reduced by one-third to half if prior to the opening of the first instance trial:

  - ✓ the Entity fully compensated for the damage caused and removed the harmful or dangerous consequences of the crime or, in any event, effectively exerted itself to said extent;
  - ✓ an organisational Model fit to prevent crimes similar to those which have taken place has been adopted or implemented.

  Furthermore, the pecuniary sanction shall be reduced by half if:

[2] Therefore, the sanction ranges between a minimum of Euro 25,823 and a maximum of Euro 1,549,370, save for corporate crime, whose pecuniary sanctions are doubled based on the provisions of the Savings Law (*i.e.* Law No. 262/2005), article 39, paragraph 5.

- ✓ the perpetrator of the crime committed the wrongful act prevalently in his/her own interest or in that of third parties and the Entity did not obtain any benefit whatsoever or obtained a minimum benefit therefrom;
- ✓ the patrimonial damage caused is of minor nature.

The fundamental principle guiding the entire subject matter of the Entity's liability sets forth that solely the Entity shall be under the obligation to pay the pecuniary sanction imposed on the Entity itself, with its own assets or common fund. The rule thus excludes any direct debt liability whatsoever on the side of the shareholders or of the members, as the case may be, regardless of the legal nature of the collective Entity.

- Bans: they shall be inflicted, together with a pecuniary sanction, only if expressly foreseen for that criminal offence and only when at least one of these two conditions arises:
  1. the company has already committed an offence resulting from a crime in the past (reiteration of offences);
  2. the company has obtained considerable profit from the crime.

  The above would lead to the following:
  a) ban from doing business;
  b) suspension or revocation of authorisations, licences or grants instrumental to the commission of the offence;
  c) prohibition to enter into contracts with the Public Administration;
  d) exclusion from concessions, funding, grants-in-aid, subsidies and possible revocation of those already granted;
  e) prohibition to advertise goods or services.

  The bans shall not be inflicted (or shall be revoked, if already inflicted as a precautionary measure) if the Entity did the following prior to the opening of the first instance trial:
  a) compensated for damages or repaired the damage caused;

b) removed the harmful or dangerous consequences of the crime (or, at least, exerted itself to that extent);
c) made the profit of the crime available to the Judiciary for seizure purposes;
d) removed the organisational deficiencies having entailed the crime, by adopting organisational models fit to prevent the commission of new crimes.

- Seizure: it consists in the State's acquisition of the price or the profit of the crime, also by way of equivalent measures (namely, by seizing an amount of money, goods or other benefits for a value corresponding to the price or profit of the crime); the seizure is always ordered with the conviction.

- Publication of the judgment: this may be ordered by the Judge when a ban is inflicted on the Entity. It takes place by affixing the judgment in the municipality where the Entity has its principal place of business, as well as by publishing it on the Internet Website of the Ministry of Justice.

- Precautionary measures: the Public Prosecutor may request that bans be also inflicted as a precautionary measure, if:
  a. there is serious circumstantial evidence as to the Entity's liability;
  b. there are grounded and specific facts such as to believe that there is an actual danger that offences of the same type as that already committed could be committed.

1.4 Exemption from administrative liability

In introducing the aforesaid administrative liability regime, the Decree foresees a specific form of exemption from any such liability should the Entity prove to have adopted all appropriate and necessary organisational measures for the purpose of preventing the commission of crimes by any persons acting on its behalf. The existence of an adequate organisation is therefore a criterion and also evidence

of the Entity's due diligence in carrying out its own activities, in particular, with respect to those in which there is a risk of committing the crimes provided for under the Decree.

The Board of Directors has the duty to adopt and to effectively implement the Organisation, Management and Control Model (hereinafter, the "OMM"), pursuant to article 6, paragraph 1, letter a), as well as to appoint the members of the Supervisory Body, pursuant to letter b) thereunder.

The Decree specifies the constituents of a successful and effective organisational apparatus which, if correctly arranged, would lead to exclude its own liability. In particular, the Entity shall be released from the relevant sanction if it proves:

- to have adopted and effectively implemented, prior to the commission of the wrongful act, organisation and management models (hereinafter, the "Model") fit to prevent crimes similar to those which have taken place;
- to have entrusted a body within the Entity having independent initiative and control powers with the supervision over the implementation of and compliance with the Model, as well as with the duty to ensure that it is updated (hereinafter, the "Supervisory Body");
- that the persons having committed the crime did so by fraudulently evading the Model;
- that there has been no omitted or insufficient supervision by the Supervisory Body.

Furthermore, article 6, second paragraph, also mentions the Model's content, which must have the following characteristics:

a) identify the activities within the scope of which there is a possibility that the crimes under the Decree are committed;
b) foresee specific protocols aimed at planning the training and the implementation of the Entity's decisions in connection with the crimes to be prevented;
c) identify ways of managing the financial resources fit to prevent the commission of any such crimes;

d) foresee obligations to inform the Supervisory Body;
e) introduce an internal disciplinary system fit to impose a sanction on the failure to abide by the measures mentioned in the Model.

The Decree foresees that the Models may be adopted, ensuring the requirements above, based on codes of conduct (also called guidelines) drafted by the trade associations.
The guidelines are communicated to the Ministry of Justice which, in agreement with the competent Ministries and within 30 days, may raise its remarks on whether the Models drawn up in compliance with the guidelines of the trade associations are fit to prevent the crimes.

2. Adoption of the Model

2.1 Aims pursued by adopting the Model

By adopting, effectively implementing and constantly updating the organisational model under Legislative Decree No. 231/2001, Banca Sistema S.p.A. (hereinafter, the "Bank") undertakes to act in conditions of fairness and transparency in carrying out the company's business and activities.

Banca Sistema is an independent banking institution, incorporated in June 2011 as a result of the integration between the business of Banca Sintesi S.p.A. and that of S.F. Trust Ltd. Group, specialised in the purchase and management of trade receivables claimed by companies against the Italian Public Administration. The Bank has been listed on the Italian Equities Market (MTA) – STAR Segment, organised and managed by Borsa Italiana S.p.A. since July 2015.
From the very beginning of its business, the Bank has expanded its own activities and services offered to its business and retail customers, by putting the factoring and debt collection products together with the full range of banking services, by opening new branches and increasingly improving Customer customisation,

ranging from large multinationals to small and medium-sized enterprises, besides professionals and savers.

One of the main aims pursued by Banca Sistema is not only that of meeting the financial demand of companies, serving as a link between the public and private sectors, as well as favouring its efficiency and a correct balance of financial demand, but also that of ensuring that companies and persons have access to an evolved, simplified and available banking world, which also listens carefully to the needs of a Country and of entrepreneurs that are growing.

The Bank is capable of offering a wide range of services, that is without recourse and with recourse factoring (also between individuals), reverse/maturity factoring, reimbursement of VAT credits, certification of receivables of the Public Administration, current accounts, fixed deposit accounts for a duration up to 10 years, salary-backed loans/pension-backed loans and pawn loans.

The Bank is also actively involved in the sector of the purchase and management of overdue financial and commercial receivables, as well as in debt management and collection between private persons, thanks to the strategic minority shareholding in other companies.

Aware of the need to ensure conditions of fairness and transparency in carrying out the company's business and activities, in order to protect its own position and image, as well as the expectations of its own employees, Banca Sistema has deemed that the implementation of the Model under Legislative Decree No. 231/2001 meets its own company policies.

Such initiative has been taken upon the firm belief that the adoption of the Model – beyond the rules under the Decree, which mention that the Model is an optional and, thus, non-compulsory element – may be a valid instrument for raising the awareness of all those who act in the name and on behalf of the Bank, in order for them to hold correct and consistent behaviours in carrying out their own activities, such as to prevent the risk of committing the crimes foreseen by the Decree.

The aforesaid Model has been prepared by considering not only the rules under the Decree, but also the guidelines on the subject matter drawn up by the trade associations (e.g. Confindustria and Assiosim).
By still implementing the provisions under the Decree and in adopting any such Model, the Board of Directors has instructed a Supervisory Body (hereinafter, the "SB") to assume the duties of a control body, with the task of supervising over the implementation of, effectiveness of and compliance with the Model, as well as of taking care that it is updated.

2.2 Corporate governance model

The Bank's corporate governance model is structured in such a way as to ensure and guarantee the maximum operational efficiency and effectiveness, by adopting the so-called 'traditional' management and control system. According to such model, management falls within the exclusive scope of authority of the Board of Directors, supervision falls within the exclusive scope of authority of the Board of Statutory Auditors, whilst auditing falls within the exclusive scope of an auditing firm enrolled in the special register held by Consob.

The Shareholders' Meeting is the body which represents the totality of shareholders and which has the authority to resolve, (i) by way of the relevant Ordinary Shareholders' Meeting, on the approval of the annual financial statements, on the appointment and revocation of the members of the Board of Directors, on the appointment of the members of the Board of Statutory Auditors and of the respective Chairperson, on the calculation of the fees of Directors and Statutory Auditors, on the granting of the auditing mandate, on the liability of Directors and Statutory Auditors, and on any further matters falling within its own scope of authority; (ii) by way of the relevant Extraordinary Shareholders' Meeting, on the amendments to the Articles of Association and on any extraordinary transaction, such as capital increases, mergers and spin-offs, save for whatever may be delegated to the Board of Directors under the Articles of Association pursuant to law.

The Board of Directors is the body invested with full powers for ordinary and extraordinary management purposes, and fulfils the entire duties provided for by law and by the Self-Regulation Code.

The Board of Statutory Auditors is the body in charge of supervising over the compliance with the law and with the Articles of Association, the compliance with the principles of correct management, the suitability of the internal control system, as well as of the organisational, administration and accounting structure, and over its reliability. Furthermore, it is requested to supervise over the specific implementation of the corporate governance rules adopted by the Company and to supervise over the independence of the auditing company. Following the entering into force of the Consolidated Law on Statutory Auditing, the Board of Statutory Auditors fulfils further and/or strengthened supervisory duties in the capacity as "Committee for internal control and auditing".

The Board of Statutory Auditors is composed of three standing statutory auditors and of two alternate statutory auditors, who will remain in office for three financial years; in no way may the Statutory Auditors assume offices in bodies other than those of control at other companies belonging to the Group or to the financial conglomerate, as well as at other companies in which the Bank holds a strategic shareholding, also indirectly.

Furthermore, in compliance with the recommendations given under the Self-Regulation Code of listed companies to which the Bank has adhered and with the corporate governance principles complied with at international level and recommended at European level, the Board has set up the following Committees inside the Board of Directors itself:

- Internal Board Committees, amongst which, the following are included:
  - Executive Committee
  - Committee for Internal Control
  - Appointments Committee
  - Remuneration Committee
  - Ethical Committee
- External Board Committees:

- Managing Director's Committee
- Risk Management Committee
- Technical and Organisational Committee

The statutory auditing of the accounts is carried out by an auditing firm enrolled in the special register held by Consob. The Shareholders' Meeting has the duty to appoint said firm, upon the grounded proposal of the Board of Statutory Auditors, pursuant to section 2409 *bis et seq.* of the Civil Code and to Legislative Decree No. 39 of 27 January 2010.

2.3 The proxy and power of attorney system

The Bank's policy foresees that only persons vested with formal and specific written powers of attorney may undertake obligations towards third parties in the name and on behalf of the Bank itself. Therefore, the latter has adopted a proxy and power of attorney system which is consistent with the assigned organisational responsibilities implying effective needs for representation foreseeing, if necessary, precise reference to quantitative thresholds of expenditure fixed by internal company regulations.

Corporate proxies shall normally mean two different concepts:

1. Proxies to the Directors

The Board of Directors may assign its own powers to one or more directors (who, following the granting of the relevant proxies, shall become Managing Directors or Directors with a proxy). All proxies are approved by the Board of Directors and the relevant minutes are filed with the Chamber of Commerce, in order to inform third parties on the contents of the proxies.

2. Appointments to specific functions within the Bank

Appointments to specific functions are an organisation of the powers inside the Bank, above all, coming from company law scholars and taken from case law, mainly, of criminal law nature (cf. Legislative Decree No. 81/2008 and laws and regulations on the environment). Through the appointments to specific functions, the Board of Directors and/or the Managing Director/s assign the internal

organisational powers to top management and throughout the entire company structure. The appointments to specific functions do not entail any "acting in the name and on behalf of the Bank" whatsoever.

3. Powers of attorney

When the fulfilment of an act entails an "acting in the name and on behalf" of the Bank (that is, the act reverberates outside), the relevant power, unless if falling with a director, must be granted through a power of attorney. The power of attorney is therefore the instrument based on which the powers to fulfil acts outside are granted to employees or to third parties, non-directors. In order for the granted powers to be enforced against third parties, the power of attorney shall have to be a 'notarial' power of attorney and shall be filed with the Chamber of Commerce, failing which, in no way may the Bank object any limitation of powers to the third party: should that be the case, the proxy may bind the Bank without any limitation whatsoever.

Having stated the above, generally speaking, the system for appointing specific functions and the power of attorney system adopted by the Bank ensure as follows:

- the powers are exercised within the scope of a decision-making process by positions of responsibility that are consistent with the importance and/or criticality of certain financial transactions;
- the persons who carry out the activities by proxy participate to the decision-making process;
- the powers and responsibilities are clearly defined, are consistent with each other and are known within the corporate organisation;
- the Bank is validly bound towards third parties (e.g. customers, suppliers, banks, public authorities, etc.) by a specific and limited number of persons vested with proxies formalised and duly communicated outside the company, where the relevant powers are specifically mentioned;
- the mapping of the persons (also non-employees) who have been vested with the power to bind the Company towards third parties is constantly updated.

The company departments concerned, with the support of the Supervisory Body, shall regularly check the proxy and power of attorney system in force, also by examining the documentation certifying the activity actually carried out by the persons who act on behalf of the Bank, suggesting the necessary changes in the event that the management and/or qualified functions do not meet the granted powers of representation.

3. Purpose of the Model

3.1 The Model of Banca Sistema

The main purpose of the Model is to build a structured and organic system of procedures and control activities aimed at preventing the perpetration of the different types of crimes foreseen under the Decree.

The principles and the provisions included under this Model must be complied with by the members of the Board of Directors, of the Board of Statutory Auditors, by all Bank employees, by the advisors, collaborators and, in general, by whomever acts in Italy and abroad on behalf of or in favour of the Bank in the areas at risk of '231' crime, as identified from time to time.

In particular, by identifying the areas of activities at risk and the consequent ways of carrying out the activities above, the Model sets itself the following aims:

- fix, in whomever acts in the name and on behalf of the Bank in the 'areas of activity at risk', the awareness of the possibility to incur, in the event of breach of the provisions cross-referenced therein, an offence liable to sanctions by the company as provided for under Chapter 6;
- stress that such forms of unlawful behaviour are strongly censured by Banca Sistema, since they are not only against the law provisions, but also against the ethical and social principles by which the Bank intends to abide in doing its own business;
- thanks to the monitoring over the 'areas of activity at risk', allow the Bank to promptly intervene to prevent or fight against the commission of any such crimes.

The cornerstones of the Model are, besides the principles already mentioned:

- the activity related to the raising of the awareness and spreading at all company levels of the rules of conduct and of the established procedures;
- the 'mapping of the areas of activity at risk' of the Bank, that is of the activities in which scope it is deemed that there is a higher possibility for the crimes to be committed;
- the assignment to the SB of specific supervisory tasks over the effective and correct implementation of the Model;
- the check and documentation of the transactions at risk;
- the compliance with the principle of segregation of duties;
- the definition of authorisation powers which are consistent with the assigned responsibilities;
- the check of the company behaviours, as well as of the implementation of the Model with the consequent regular update.

3.2 The Model's preliminary activity

The Model of Banca Sistema has been prepared by following the method recommended by the guidelines of the main trade associations, that is by splitting the activity into three phases:

Phase 1 - Risk analysis

Analysis of the areas at risk which may cause detrimental events pursuant to the Decree.

In particular, the risk analysis is carried out through the following methodological approach:

- analysis of the Bank's corporate and organisational structure, through the study of the main corporate documentation, aimed at reaching a general understanding of the Bank;
- understanding of the Bank's business model;

- historical analysis related to possible cases already emerged in the past in connection with criminal, civil or administrative records against the Bank or its employees having points of contact with the relevant laws and regulations;
- analysis of the specific risks which may cause detrimental events to the aims mentioned under the Decree;
- analysis and observation of the law and regulatory systems, as well as of the control systems adopted by the Bank in the areas deemed potentially at risk.

The development of the phase at issue also took place by interviewing 'key persons' of the decision-making and control system, and has been integrated in light of the Bank's listing on the stock exchange.

Phase 2 – The gap analysis

Through said activity, the control systems existing inside the Bank to protect the areas at risk identified in Phase 1 were compared with the organisational requirements requested by the Decree in order to identify all necessary changes to prepare the model aimed at preventing the 'predicate offences'.

Phase 3 – Definition of the General Part of the Model

The General Part includes an overview of the regulatory contents of the Decree and of the purposes of the Model, the identification of the Bank's Supervisory Body (of its characteristics, duties, powers and reporting system) and of the sanctioning structure arranged by the Bank for the breach of the rules of conduct provided for under the Model itself.

The Board of Directors is responsible for updating the Model and for aligning the latter as a result of any and all changes to the organisational structures, operational processes, the findings of all controls, and to the legislative amendments/integrations introduced by the legislator for the criminal offences foreseen.

Phase 4 – Preparation of the Special Parts of the Model

This part is aimed at setting out the general and specific procedural principles aimed at preventing the commission of the predicate offences.

The Special Parts under this Model concern:

- crimes against the Public Administration (articles 24-25);
- corporate crimes (article 25-*ter*);
- market abuse crimes (article 25-*sexies*);
- money laundering and terrorist crimes (article 25-*octies*);
- computer crime and unlawful data processing (article 24-*bis*).
- manslaughter and serious or very serious injury crimes committed in breach of the laws and regulations on hygiene and safety in the workplace (article 25-*septies*).

Furthermore, we would like to lay stress on the fact that some crimes have been introduced for prudential reasons, since, even if there are no specific facts from which it is possible to infer the existence of actual risks, it is the case of crimes to which the Bank in any event intends to put a high level of attention.

3.3 Approval of the Model and its implementation

The Board of Directors has been requested, also based on criteria and instructions issued to said extent, to expedite the adoption of an own Model by way of the relevant resolution to said extent, depending on the risk profiles which may be found in the activities carried out by the Bank.

In adopting the Model, the Bank's Board of Directors at the same time appointed its own Supervisory Body, in charge of fulfilling the duties of control over the carrying out of any such activities and over the application of the Model.

The Bank has the duty to prepare, adopt and update the Model in connection with the needs for alignment ascertained from time to time. In particular, the Board of Directors is requested, also upon the proposal of the SB, to integrate this Model, if necessary, by way of the relevant resolution to said extent, by integrating the predicate offences as foreseen under the laws and regulations in force from time to time.

Furthermore, the Bank is under the responsibility to apply the Model in connection with the activity actually carried out. For said purpose, the SB is assigned the primary duty to exercise the controls over the implementation of the Model in compliance with the procedures described therein.

4. The Supervisory Body

4.1 Requirements

By implementing the provisions under the Decree – which makes the granting of the exemption from administrative liability conditional upon the fact that the duty to supervise over the implementation of and compliance with the model is entrusted to one of the Entity's bodies – a collective 'Supervisory Body' (or "SB") has been identified within Banca Sistema, composed of three members, all having adequate skills and professional competence to cover any such role. The SB is composed as follows:

i. The Chairman of the Board of Statutory Auditors, in order to guarantee and ensure the adequacy of all functions involved in the internal control system, the proper performance of tasks and coordination of the functions themselves, promoting actions to correct any deficiencies and irregularities detected. The Chairman of the Board of Statutory Auditors also assumes the chair of the SB by right.

ii. An independent Board member or an external expert with a solid track record in 231 matters

iii. the Head of the Bank's Internal Audit Function, in order to guarantee a correct coordination of all audit-related activities, thus avoiding any overlap and exploiting possible internal control synergies

The SB is vested with independent initiative and control powers, aimed at ensuring an effective and successful implementation of the Model, and must meet the following requirements:

1. Autonomy: it must have decision-making autonomy, that is as an essential freedom of self-determination and action, with full exercise of the technical discretionary power in fulfilling its own duties. First, the autonomy shall be towards the other corporate bodies, top management and management, in such a way as for the SB to be able to act free from any conditioning or pressure whatsoever. The SB must also enjoy autonomy of expenditure.
2. Independence: it must be devoid of any conditioning whatsoever arising out of any bond of subjection towards the Bank's control top management and must be a third body, placed in an independent position, also hierarchical, capable of taking autonomous measures and initiatives.
3. Professional competence: it must be professionally competent and reliable, as regards both each single member composing the SB and in its entirety; as a body, it must have the necessary technical knowledge and professional competence in order to fulfil all entrusted duties in the best possible way. For said purpose, it may avail itself of the specific expertise of each single member or of other bodies and/or company functions (e.g. Risk and Compliance/Anti-Money Laundering), as well as of external advisors.
4. Continuity of action: it must fulfil all entrusted duties on an ongoing basis, even if not on an exclusive basis, by being assisted by the other control functions (e.g. Compliance/AML and Internal Audit).
5. Reputation and lack of conflicts of interest: in no way may a person in any of the following situations be appointed member of the SB and, should that be the case, any such person would forfeit office:
   - a debarred, disabled or bankrupt person or, in any event, a person who has been convicted for one of the crimes foreseen under the Decree or, in any event, sentenced to disqualification, even temporary, from holding public offices or to legal incapacity to hold any executive office;
   - a person who has business relations (understood, for instance, as partnerships, profit-sharing agreements, joint ventures, etc.) with the Bank or with the controlled or controlling companies and/or any other relation such as to jeopardise independence.

Should a member of the SB have an interest on his/her own behalf or on behalf of third parties in a resolution, the member concerned shall have to inform the other members of the Body to said extent, by specifying the nature, the terms and conditions, as well as the origin and extent. The other members shall decide whether the person concerned shall have to abstain from the resolution.

The Board of Directors shall appoint the members of the SB, who shall remain in office for three years, but may be revoked at any time for just cause by the BoD.

As regards its control functions, the SB may be assisted by external parties who carry out audit-related activities professionally.

In case of renunciation, supervening incapacity, death, revocation or forfeiture of a member of the SB, the Board will replace it at the first useful session.

In any case, the outgoing member remains in office until the new member has been appointed by the Board.

The Chairperson shall coordinate the Body's work and shall ensure that all members are adequately informed on all the issues under the Agenda.

The SB has adopted its own regulation governing its operation.

4.2 Procedure to convene and to hold the meetings of the SB

The SB shall meet whenever the Chairperson or one of the members deems it expedient, or if so requested by the Board of Directors or by the Board of Statutory Auditors and, in any event, at least every six months.

All SB meetings shall be held in the venue mentioned in the notice of call, making reference to the date, time and venue of the meeting, as well as to the list of issues to be dealt with. The notice of call, to be communicated to each single Body member (by email, fax or by hand delivery), must be sent at least three days prior to the date scheduled for the meeting or, if urgent, at least one day beforehand.

SB meetings may also be held by audio and/or videoconference, provided that all persons attending may be identified and are enabled to follow the discussion and to take part in the dealing with the issues and in the voting.

The decisions of the SB on the matters at issue may be adopted through written consultation or through express written consent.

Such resolutions, as well as the reports related to the audits carried out by the Body, either directly or through external collaborators, shall be recorded into the Body's Meetings Ledger, filed with the Bank's offices.

4.3 Duties and powers of the SB

The SB of Banca Sistema is independent from the corporate bodies and is free from any bond of hierarchical subordination.

The persons/bodies to whom the SB reports within the company are, on an ongoing basis, the Managing Director and the Heads for the control functions of the Bank and, on a regular basis, the Board of Directors and/or the Board of Statutory Auditors.

The Bank's SB may be called at any time by the aforesaid bodies - or may in turn submit a request to said extent - to report in connection with the implementation of the Model or with specific situations.

Furthermore, at least on an annual basis, the SB shall provide the Board of Directors and the Board of Statutory Auditors with a written report on the activities carried out and on the implementation of the Model.

In order for the Supervisory Body to fulfil its duties, the latter is vested with full financial and managerial independence, without any expenditure limits whatsoever. The Body shall promptly inform the Bank's BoD should it engage considerable resources to face exceptional and urgent situations.

The Supervisory Body of Banca Sistema is entrusted with the duty to supervise:

- over the implementation of and compliance with the rules under the Model by the recipients, specially identified in the specific Special Parts in connection with the different types of crimes foreseen under the Decree;
- over the actual effectiveness and effective capability of the Model, as regards the company structure, to prevent the commission of the crimes under the Decree;

- over the expediency of updating the Model, should it be deemed necessary to align the latter due to changed company conditions.

From a practical standpoint, the SB has the duty to:

- implement all control procedures, bearing in mind that the primary responsibility for controlling the activities, also for those areas of activity at risk, falls with the operational management and forms an integral part of the business process, which confirms the importance of a staff training process;
- investigate the company's business for the purposes of an updated mapping of the areas of activity at risk within the business context;
- carry out regular checks aimed at certain transactions or specific acts implemented within the scope of the areas of activity at risk as defined in the specific Special Parts of the Model;
- promote adequate initiatives for spreading the knowledge and understanding of the Model, and prepare the necessary internal organisational documentation for the purpose of implementing the Model, including the relevant instructions, clarification or updates;
- collect, process and keep the significant information (including the notifications under paragraph 4.5 below) in connection with the compliance with the Model, as well as update the list of information to be compulsorily sent to the SB or made available to the latter;
- coordinate with the other company functions (also through specific meetings to said extent) for better monitoring the activities in the areas at risk. For said purpose, the SB shall be kept constantly informed on the development of the activities in the aforesaid areas at risk and shall have free access to the entire relevant company documentation. Management shall also report to the SB any possible situations of the company's business which may expose the Bank to the risk of commission of a crime;
- control the actual existence, the regular keeping and effectiveness of the documentation requested in compliance with the provisions of the specific Special Parts of the Model for the different types of crimes. In particular, the SB shall be informed of the most significant activities or of the transactions

foreseen under the Special Parts, and shall be provided with all documentation update related data, for the purposes of enabling all controls;

- carry out internal investigations in order to ascertain alleged breaches of the rules under this Model;
- check that the elements foreseen under the specific Special Parts of the Model for the different types of crime (adoption of standard clauses, completion of procedures, etc.) are in any event adequate and meet the needs for complying with the rules under the Decree, otherwise updating any such elements;
- constantly liaise with the other control bodies (Board of Statutory Auditors and the Internal Control Committee), with the auditing firm and with the internal control functions;
- coordinate with the heads of the other company functions for the different aspects related to the implementation of the Model (definition of standard clauses, training of staff, disciplinary measures, etc.).

4.4 Information flows towards the Supervisory Body

Pursuant to article 6, paragraph 2, letter d), of the Decree, the SB must be promptly informed by all Model recipients in connection with any information on the existence of possible breaches of the Model. In particular, Model recipients must report any information on the commission or possible commission of crimes or of behavioural deviations from the principles included in the Model.

In any event, the SB must be provided with information:

a) which may pertain to potential breaches of the Model such as, by way of example:
   - possible offers or requests of money, of gifts (in excess of the respective reasonable value), or of other benefits coming from or aimed at public officials or persons in charge of a public service;
   - orders and/or information coming from investigation police bodies, or from any other authority, from which there is evidence as to the carrying

out of investigations for the offences, also against persons unknown, should such investigations involve the Bank and/or its top management and/or employees;

- requests for legal assistance submitted by top management in the event of commencement of legal proceedings for the crimes;
- information related to the sanctioning proceedings commenced by the Public Authorities and to any possible measures inflicted (including orders against top management) or the decisions to dismiss any such proceedings with the relevant grounds, should they be linked to the commission of crimes or to the breach of behavioural or procedural Model rules;
- expenditure anomalies arising out of authorisation requests;
- possible omissions or carelessness in the bookkeeping on which the accounting entries are based;
- any notification, not promptly checked by the competent functions, concerning both any deficiency or unsuitability of the workplace or work tools, or of the protection devices made available to the Bank, and any other dangerous situation connected with safety at work.

b) Information pertaining to the duties of the SB and which may be important for fulfilling its duties such as, for instance:

- the information related to the Bank's organisational changes;
- the reports prepared by the different functions in connection with the activities deemed related or which may be deemed related to the Bank's areas at risk;
- the annual financial statements, inclusive of the notes to the financial statements and statement of financial position;
- the communications prepared by the Board of Statutory Auditors and by the Auditing Firm on any criticalities found, even if solved.

The Supervisory Body ensures the maximum confidentiality in connection with any news, information, notification, subject to revocation of the mandate and of the disciplinary measures set out in this document, without prejudice to the

needs pertaining to the carrying out of the investigations should it be necessary to be assisted by external advisors or by other corporate structures.

The top managers and subordinates pursuant to art. 5 lett. a) and b) of the Decree may present, to protect the integrity of the Entity, detailed notifications of which they have come to know due to the functions and related to:

a) unlawful conducts relevant to the Decree and based on precise and concordant facts;

b) violations of the Organisational and Management Model;

These notifications must be sent using the following alternative methods:

a) to the e-mail box odv@bancasistema.it;

b) through the "whistleblowing"[3] information channel available on Intranet.

The reporting management process is governed by the Internal Whistleblowing Rules adopted by the Bank; both the aforementioned channels guarantee the confidentiality of the reporting agent's identity in the reporting management activities.

The Supervisory Body shall assess all notifications received and shall take all consequent initiatives at its reasonable discretion and under its own responsibility within its respective scope of authority by hearing, if necessary, the author of the notification and the person liable for the alleged breach. Any consequent decision shall be grounded and any consequent measures shall be applied in compliance with the provisions under Chapter 6 on the "Disciplinary System".

In compliance with the provisions of Law No. 179/2017, the Entity guarantees the authors of the notifications against any form of retaliation, discrimination, penalisation or any consequence arising therefrom, by ensuring them confidentiality on their identity, in any event, save for the obligations provided for by law and for the protection of the rights of the Bank or of the persons accused wrongly or in bad faith.

It is noted that the Art. 6 of the Decree[4], Paragraph 2-ter, provides that the adoption of discriminatory measures against individuals who make notifications referred to Par. 2-bis can be reported to the National Labor Inspectorate, for the measures within its jurisdiction. Furthermore, it provides that the retaliation or discriminatory dismissal of the reporting party, as well as the change of duties, are considered null and void (Par. 2-*quater*). It is the responsibility of the employer to demonstrate that these measures are based on reasons not related to the report itself.

Any information and notification under this Model is kept by the Supervisory Body in a special computer and paper archive, in compliance with the provisions under Legislative Decree No. 196 of 30 June 2003 (Data Protection Code).

4.5 Information flows from the Supervisory Body towards the corporate bodies

The Chairperson of the SB, or one of the other members appointed by the latter, shall inform the Board of Directors on the Model's application and implementation, as well as on any critical aspects arising, on the need for actions for change, in the event of any notification received or other urgent matters.

No later than 90 days as of the closing of the financial year, the SB shall draw up a report summarising the activity carried out throughout the previous year, together with an action plan for the current year, to be submitted to the Board of Directors.

4.6 Rules of operation of the SB

The SB shall schedule all periodic control activities depending on the state of the company's activities and on the available information.

[3] The Board of Directors has appointed the Head of the Internal Audit function of the Bank as responsible for whistleblowing reports.

[4] The Law No. 179 dated 15 November 2017 introduced in the Legislative Decree No.231/2001 the whistleblowing rules, that is to say the reporting of illegal activities or violations related to the Model by the employee or collaborator who has come to know about it for work reasons.

The annual action plan shall be approved by the SB at the beginning of each financial year, mentioning the areas and functions to be checked and the relevant criteria. The checks may be carried out by the members of the SB, or be entrusted to the Internal Audit Department or to external advisors.

A report shall be prepared at the end of each check, describing the activities and the respective findings. The following shall be mentioned amongst the findings:

- the company areas checked and any further useful information;
- the level of compliance or the criticalities found compared to the audit's criteria;
- the cross-reference to the control documentation;
- any recommendations;
- any other information deemed expedient for a better assessment of the checked activity.

The findings of the activities shall be examined at the following meeting of the SB. If deemed expedient, the SB may carry out further in-depth checks, also with the assistance of external advisors, or request the Bank's management body to act in order to take the level of risk back to acceptable levels.

The SB's recommendations shall be promptly followed by the functions concerned and the Board of Directors shall have the duty to check that they are effectively applied.

The SB shall request regular meetings with the Board of Statutory Auditors and with the internal control functions to share the strategies for implementing the internal control system, avoiding any overlap and exploiting any and all synergies.

5. Communication plan

5.1 Introduction

In order to effectively implement the Model, it is the Bank's intention to ensure that the contents and principles therein are correctly disseminated both inside and outside the corporate structure.

In this respect, the Bank aims at extending the communication of the Model's contents and principles not only to its own employees, but also to any person contributing, even occasionally, to the achievement of the Bank's aims under the relevant contracts and working under the Bank's management or supervision (e.g. collectors).

Although such communication activity is characterised in a different way, depending on the recipients to whom it is aimed, the information concerning the Model's contents and principles shall in any event be marked by completeness, timeliness, accuracy, accessibility and continuity, in order to allow the different recipients to be fully aware of all those company instructions that are required to comply.

In particular, the SB promotes appropriate initiatives for the dissemination of knowledge and understanding of the Model to the interested parties.

5.2 Spreading and training

The Model's contents and principles shall be disclosed to all employees and to all other persons liaising with the Bank under the relevant collaboration agreement.

All employees are under the obligation to:

i) become aware of the Model's contents;
ii) know the operational procedures with which their own activity is to be carried out;
iii) as regards the respective role and responsibilities, actively contribute to effectively implementing the Model, thus reporting any deficiencies found therein.

In order to ensure an effective and rational communication activity, the Bank promotes and facilitates the knowledge of the Model's contents by all employees, with a diversified level of in-depth analysis depending on the level of involvement in the activities identified as sensitive pursuant to the Decree.

All employees are ensured the possibility to access and consult the Model, the Code of Ethics, as well as the company's internal rules and regulations (procedures, regulations, policies, etc.).

Furthermore, in order to make the understanding of the Model easier, all employees are under the obligation to take part in all training activities, in different ways depending on their level of involvement in the activities identified as sensitive pursuant to the Decree.

A USB key shall be given to all new employees upon their hiring, including a copy of the internal rules and regulations in force. All new employees must sign a declaration of compliance with the Model's contents.

The same rules for spreading the Model foreseen for employees shall apply to the members of the corporate bodies of Banca Sistema.

Adequate communication tools shall be adopted to update all employees on the amendments, if any, made to the Model, as well as on any important procedural, law, regulatory or organisational change.

The activity aimed at communicating the contents of the Model and of the Code of Ethics is also aimed at those third parties liaising with the Bank under the relevant collaboration agreement or representing the Bank without any bond of employment (for instance, commercial partners, introducers, agents in financial activity, credit intermediaries, financial promoters, advisors, business agents and other independent collaborators).

For said purpose, Banca Sistema shall provide the most significant third parties with a Model and with a copy of the Ethical Code. Furthermore, they shall also be requested to sign a declaration acknowledging receipt of any such documents, together with the undertaking to comply with the contents described therein.

The OMM and the Code of Ethics are available on the Company's Website www.bancasistema.it under the section "Useful Links".

The knowledge by all Banca Sistema employees of the principles and provisions under the Model is of primary importance for effectively implementing the Model.

Banca Sistema runs specific training activities aimed at all employees, with the support of the company functions in charge - assisted, if necessary, by external

advisors with professional competence in the matter of the administrative liability of entities - in order to ensure an adequate knowledge, understanding and spreading of the Model's contents and to also spread a business culture aimed at pursuing greater transparency and ethicality.

The contents of the training activities are constantly updated in connection with any necessary update of the Model.

It shall be compulsory to attend all training activities, and the SB shall collect and file all evidence/certificates concerning the effective participation to any such training activities.

6. Disciplinary system

6.1 General principles

The organisation of an adequate sanctioning system for the breach of the rules under the Model is essential to ensure its effectiveness and in order for the SB's action to be efficient.

Indeed, in said respect, article 6, paragraph 2, letter e), of the Decree foresees that all organisation and management models must "*introduce a disciplinary system fit to sanction the non-compliance with the measures mentioned in the Model*".

The disciplinary sanctions shall be inflicted regardless of the outcome of the criminal proceedings, if any, since the Bank undertakes the rules of conduct imposed by the Model in full autonomy and regardless of the type of offence which the breaches of the Model may entail.

The breaches may also be ascertained on the initiative of the SB, after having detected a possible breach of the Model in carrying out its control and supervisory activity.

The Managing Director or, as the case may be, the Human Resources Function shall have the authority to inflict sanctions on the relevant executives, senior managers and employees.

The SB may also be requested to fulfil an advisory function throughout the entire disciplinary procedure, in order to get any necessary useful evidence in view of constantly updating the Model. Any liability arising out of the breach of the Model and the infliction of the consequent sanction shall in any event be ascertained in compliance with the laws and regulations in force, with data protection, with dignity and with the reputation of the persons involved.

The disciplinary system is constantly monitored by the Supervisory Body and by the Human Resources Function.

6.2 Measures against the Directors

The Bank assesses with the utmost strictness the breaches of this Model by whomever is in the Bank's top management and, therefore, where there is an exposure to the image towards the employees, shareholders, creditors and the public. The training and the consolidation of business ethics sensitive to the values of fairness and transparency implies, above all, that said values are embraced and complied with by whomever leads the company's choices, in such a way as to be an example and stimulus for all those working for the Bank at all levels.

Should the Directors breach the internal procedures and the principles of conduct provided for under this Model and/or should they take measures in fulfilling their own duties against the provisions or principles under the Model, the SB shall promptly inform all the members of the Board of Directors and of the Board of Statutory Auditors who, depending on their respective scope of authority, shall take the most expedient and adequate initiatives consistently with the seriousness of the breach and in compliance with the powers provided for by law and/or under the Articles of Association (e.g. statements in the minutes for the meetings, convocation of the Shareholders' Meeting in order to resolve upon the measures against the persons liable for the breach, amongst which, the revocation of the appointment as director and the bringing, if necessary, of the liability actions provided for by law).

6.3 Measures against the members of the Board of Statutory Auditors

As regards the members of the Board of Statutory Auditors, the breaches of the rules under this Model shall be promptly reported to the SB, to all members of the Board of Statutory Auditors and to all members of the Board of Directors. After having heard the opinion of the Board of Directors, the Board of Statutory Auditors shall take all necessary measures against the Statutory Auditors having committed the charged breaches.

6.4 Sanctioning system against the executives

In the event of breach of the provisions and rules of conduct included in the Model by any executives, since the relevant collective bargaining agreement does not foresee any 'conservative' disciplinary measure given the special nature of the fiduciary bond of any such category of employees, the Bank may assess that the aforesaid breaches amount to adequate grounds for terminating the employment contract with any such executive.

6.5 Sanctioning system against the employees

The behaviours held by the employees (excluding the executives) in breach of specific rules of conduct inferred from this Model are defined as disciplinary offences.

The sanctions which may be inflicted on said employees fall amongst the sanctions provided for under Law No. 300/1970, amended by Law No. 92 of 28 June 2012, and under the relevant provisions under the banking collective bargaining agreement in force.

Insofar as the above is concerned, the Model refers to the categories of wrongful acts which may be sanctioned foreseen under the sanctioning system mentioned above. Such categories describe the sanctioned behaviours, depending on the

importance of each single case considered and the sanctions foreseen in practice for the commission of the wrongful acts depending on their seriousness.

Should any employee breach the internal procedures foreseen by this Model or adopt a behaviour in breach of the rules under the Model and under the Code of Ethics in carrying out his/her own activities, whereby it shall be necessary to recognise a breach of the relevant contract in any such behaviours, entailing a detriment to the company's discipline and morals, the disciplinary measures foreseen in connection with the seriousness or recidivism of the offence or with the level of negligence shall apply, namely:

a. any employee breaching one of the internal procedures foreseen under this Model or adopting a behaviour in breach of the rules of the Model shall incur the 'verbal reprimand' measure;
b. any employee who is recidivist in breaching the procedures foreseen under the Model or in adopting a behaviour in breach of the rules of the Model shall incur the 'written reprimand' measure;
c. any employee causing damage or creating situations of potential danger for the Bank in breaching the internal procedures foreseen under the Model or in adopting a behaviour in breach of the rules of the Model in carrying out activities in the sensitive areas, or any employee committing the offences under paragraph b) above with recidivism, shall incur the 'suspension from work and from salary' measure (for a maximum of 10 days). Such behaviours, held due to the non-compliance with the instructions given by the Bank, could entail damage to the Bank's assets and/or amount to acts against the Bank's interests and/or exposing the Bank to risks of administrative sanctions or bans;
d. any employee adopting a behaviour in carrying out his/her own activities in the sensitive areas in breach of the rules of the Model and amounting to considerable breach, unequivocally aimed at perpetrating a crime sanctioned by Legislative Decree No. 231/2001 or entailing the actual application against the Bank of the measures foreseen under Legislative Decree No. 231/2001 shall incur the 'termination of the employment

contract for justified subjective reasons' measure; such behaviour is a considerable breach of the instructions given by the Bank and/or a serious breach of the employee's obligation to contribute to the Bank's performance;

e. any employee adopting a behaviour in breach of the rules of the Model and amounting to serious breach in carrying out his/her own activities in the sensitive areas, unequivocally aimed at perpetrating a crime sanctioned by Legislative Decree No. 231/2001 or entailing the actual application against the Company of the measures foreseen under Legislative Decree No. 231/2001, as well as any employee committing the offences under paragraph 3, first part, with recidivism shall in incur in the 'termination of the employment contract for just cause' measure. Such behaviour utterly destroys the Bank's trust in the employee, thus amounting to serious damage for the company.

The type and extent of the sanctions cross-referenced above inflicted on the employees shall consider, in practice, the principle of proportionality foreseen under section 2106 of the Civil Code, considering for each case in point:

- the wilfulness and the level of reiteration of the behaviour, the level of negligence, imprudence or carelessness, also in connection with the predictability of the event;
- the objective seriousness of the wrongful act amounting to a disciplinary offence;
- the employee's overall behaviour, in particular, as regards the existence of previous disciplinary records or not, to the extent permitted by law;
- the employee's tasks;
- the functional position of the persons involved in the wrongful acts amounting to the offence;
- the other specific circumstances coming with the disciplinary breach.

By way of example but without any limitation whatsoever, the following behaviours shall amount to disciplinary offences:

- the breach of the principles and procedures provided for under this Model or set forth for its implementation, also with omissive behaviours and, if necessary, in collaboration with others;
- the drafting of false documentation, if necessary, in complicity with others;
- facilitating the drafting of false documentation by third parties through an omissive behaviour;
- the omitted drafting of the documentation requested by this Model or by the procedures set forth for its implementation;
- the removal, destruction or modification of the procedure-related documentation to avoid the control system foreseen by the Model;
- the hindrance to the supervisory activity of the SB or of the persons of whom the latter avails itself;
- preventing the access to the information and documentation requested by the persons in charge of controlling both the procedures and the decisions;
- the holding of any other behaviour fit to avoid the control system foreseen under the Model.

The Head of the Human Resources Function is responsible for the actual application of the disciplinary measures described above, who shall inflict the sanctions upon the notification of the Supervisory Body to said extent, if any, also after having heard the opinion of the manager of the perpetrator of the censured behaviour. In any event, the Supervisory Body has the duty, in collaboration with the Head of the Human Resources Function, to check and assess the suitability of the disciplinary system pursuant to and to the extent of Legislative Decree No. 231/2001.

6.6 Measures against external collaborators

All behaviours held by other Recipients, outside the Bank, such as self-employed workers, professionals, advisors, suppliers and commercial partners, against the conduct guidelines mentioned in this Model and such as to entail the risk of perpetrating a crime sanctioned by the Decree may entail the termination of the

contract, thanks to the implementation of the relevant clauses included in the contracts.

The Head of Legal and Corporate Affairs Division is in charge of drawing up, updating and including such specific contractual clauses in the engagement letters or in the partnership agreements, which shall also foresee a possible request for damages as a result of any and all damage caused to the Bank from the Judge's application of the measures provided for under the Decree.

SPECIAL PART

Purpose of the Special Part

The purpose of this Special Part is to ensure that all recipients of the Model (such as, for example, the Bank's employees, executive managers, directors, liquidators, advisors, financial agents, financial promoters, credit brokers, suppliers, contractors, introducers and partners, and in general all those who are bound to comply with this Model, hereinafter the "Recipients") adopt rules of conduct in accordance with the provisions hereof, in order to prevent any of those offences considered herein being committed.

Specifically, the purpose of this Special Part is to:

a. describe the general and specific procedural principles that the Recipients of the Model are bound to observe in order that the Model be correctly applied;
b. supply the Supervisory Body with the working instruments required to carry out the control and audit operations provided for in the Model.

Italian Legislative Decree no. 231/2001 identifies certain types of offence which if committed by persons in a position of seniority within the Bank, or by persons subject to the latter's management or supervision (Sections 6-7), constitute a source of liability for the Entity if committed in the interests, or for the benefit, of such.

Given the nature of the business carried out by Banca Sistema, the following offences, provided for by Italian Legislative Decree no. 231/2001, have been deemed of relevance – that is, potentially at risk of being committed in the interests, or for the benefit, of the company – for the purposes of the preparation of this Model:

A) Crimes against the Public Administration (Art. 24 and 25)

B) Corporate crimes (Art. 25-*ter*)

C) Market abuse offences (Art. 25-sexies)

D) Occupational health and safety offences (Art. 25-*septies*)

E) Money-laundering crimes (Art. 25-*octies*)

F) Computer crimes and unlawful data processing offences (Art. 24-*bis*)

In the light of the aforementioned considerations, the relevance of the other underlying offences identified by Italian Legislative Decree no. 231/2001 and reported in Chapter 1.2 of the General Part of this Model, has been deemed of a limited entity. In fact, it has been deemed that the risk of commission of such further offences by a person working in the Bank, during the carrying out of said person's duties in the interests and/or for the benefit of the Bank, is highly unlikely even in theory.

In any case, this Model and the Bank's entire internal control system do not fail to take account of these types of offence, and thus the rules of conduct set out in the General Part of the Model, and in Banca Sistema's Code of Conduct, shall apply, and consequently the internal control system already adopted shall continue to apply without the need to organize any further specific procedural arrangements.

Therefore, this Special Part of the Organization, Management and Control Model is divided into sub-sections that take exclusive account of the diverse types of offence mentioned above.

A) CRIMES AGAINST THE PUBLIC ADMINISTRATION

During the course of their business operations, companies may come into contact with the Public Administration. Such companies include those that tender for contracts, apply for authorizations, concessions or licences, participate in procedures for the granting of public loans, or that provide services or carry out work for the Public Administration.

The term "Public Administration" means, very briefly, any Public Entity or Person (and sometimes even those of a private nature) that performs in some way a public function in the interests of society, and thus in the public's interest. For example, the following entities or categories of entity are part of the Public Administration:

- schools and colleges of all kinds and levels, and other educational institutions;
- autonomous State entities and administrations (such as, for example, Ministries, the Chamber of Deputies and the Senate, the Department of EU Policies, the Market Regulatory Authority, the Electricity and Gas Board, the Communications Regulatory Authority, the Bank of Italy, CONSOB – the Italian Financial Markets Supervisory Authority, the Personal Data Protection Authority, the Italian Revenue Agency, ISVAP – the Italian Supervisory Authority for Private Insurance, COVIP – the Italian Supervisory Commission for Pension Funds, and bankruptcy courts);
- Regional Governments;
- Provincial Governments;
- Political parties and associations connected to such;
- municipalities and municipal companies;
- Mountain communities and their consortia and associations;
- Chambers of Commerce, Industry, Crafts and Agriculture, and their associations;
- all non-economic national, regional and local public entities (such as, for example, INPS, CNR, INAIL, INPDAI, INPDAP, ISTAT, ENASARCO);
- Local Health Authorities, Hospital Authorities, and other Public Entities belonging to the National Health System;
- State Entities and Monopolies;
- Private entities providing a public service (for example the Italian Broadcasting Company - RAI);
- Pension funds or sickness funds connected to such;
- social welfare and healthcare foundations.

Without prejudice to the purely exemplificative nature of the aforementioned public entities, it should be pointed out that not all natural persons who operate in the sphere in relation to the aforesaid entities are persons liable of criminal offences against the Public Administration.

Pursuant to Article 357, paragraph 1, of the Criminal Code, a public official "for the purposes of criminal law" is a person who exercises "a public legislative, judicial or administrative function".

The provision in question only clarifies the notion of "public administrative function" (since the other two have not led to any doubts regarding their interpretation), specifying that for the purposes of criminal law "an administrative function is public when governed by the provisions of public law, and by authoritative acts, and is characterized by the formation and expression of the will of the Public Administration, or by being carried out by means of authoritative or certifying powers".

In other words, the administrative function is considered "public" when governed by "the provisions of public law", that is, those provisions designed to pursue a public purpose and safeguard a public interest, and as such are opposed to the provisions of private law.

In a different way, Article 358 of the Criminal Code defines the "persons appointed to carry out a public service" as those persons "who in any way provide a public service. Public service means an activity governed in the same manner as the public function, but characterized by the absence of the powers that traditionally characterize the latter, and with the exclusion of the carrying out of orders received, and the provision of material services".

The legislator specifies the notion of "public service" on the basis of two criteria, one positive and the other negative. A service, in order to be considered "public", must be governed, in the same way as a "public function", by the provisions of public law, but with the difference that it does not involve any of the certifying, authorizing or deliberative powers of a public function.

Thus a public service official is a person who exercises a public office unrelated to the powers vested upon a public officer (legislative, juridical and administrative powers), and not regarding the mere carrying out of orders received and/or the provision of material services which, as such, are devoid of any intellectual or discretional contribution.

In the case of Banca Sistema, the main occasion for contact with the Public Administration is the result of the acquisition without recourse, management and collection of receivables due from the Public Administration. Equally important

are the institutional relations with the Supervisory Authorities (the Bank of Italy and CONSOB).

1 Crimes against the Public Administration

The crimes against the Public Administration governed by Italian Legislative Decree no. 231/2001 are as follows:

- **Misappropriation to the detriment of the State or the European Union (Article 316-bis of the Italian Criminal Code)**

"Whosoever outside of the Public Administration, having obtained from the State or any other Public Entity contributions, grants or funding to promote initiatives aimed at carrying out construction work or carrying out public interest activities, then fails to use said amounts for the purposes for which they were intended, shall be punished with imprisonment for a period of between six months and four years".

The crime is committed in the event that, after having obtained contributions, grants or funding from the Italian State or the European Union, the amounts obtained are not used for the purposes for which they were intended (in fact, this crime consists in the misappropriation of all or some of the amount obtained, regardless of whether or not the planned activity is actually carried out).

Bearing in mind that the moment in which the crime is committed coincides with the executive phase, the crime itself may also be committed in relation to previously obtained funding that is now not used for the purposes for which it was granted.

The crime of misappropriation could thus be committed through the utilization of funds granted at a concessional rate for purposes other than those declared.

Fines pursuant to Italian Legislative Decree no. 231/01: up to 500 units, increased by between 200 and 600 units in the event that the Entity has made a significant profit or that serious damage has been caused.

Bans pursuant to Italian Legislative Decree no. 231/01: 1) prohibition to enter into contracts with the Public Administration other than in order to obtain provision of a public service; 2) a ban on the receipt of any benefits, loans, grants or subsidies, and the possible revocation of those already granted; 3)

prohibition to advertise goods or services for a period of between three months and two years.

- **Illegal receipt of disbursements to the detriment of the State or of the European Union (Article 316-ter of the Italian Criminal Code)**

"Except when the crime is provided for under Article 640-bis of the Italian Criminal Code, whosoever utilizes or submits statements or documents that are false, or that attest to untrue things, or omits to provide due information, as a result of which they obtain grants, financing, subsidised loans or other similar contributions granted or issued by the State, by other Public Entities or by the European Union, for themselves or for others, without being entitled to them, *shall be punished with imprisonment for a period of between six months and three years. If the sum unduly received is equal to or less than 3,999.96 euro, only a fine shall be payable, said fine ranging from 5,164 to 25,822 euro. Said fine may under no circumstances exceed three times the benefit received*".

The crime is committed in the cases in which – by using or submitting false statements or documents, or by omitting due information – a party obtains grants, financing, subsidised loans or other similar contributions granted or issued by the State, by other Public Authorities or by the European Union without being entitled to them.

This crime may be committed during the phase of application for the disbursement of a loan granted (even in the form of an advance) and of the acquisition of a subsidized loan through the submission of an application containing false statements or false documents, or attesting to untrue things or omitting to include due information.

Fines pursuant to Italian Legislative Decree no. 231/01: from 100 to 500 units, increased by between 200 and 600 units in the event that the Entity has made a significant profit or that serious damage has been caused.

Bans pursuant to Italian Legislative Decree no. 231/01: prohibition to enter into contracts with the Public Administration other than in order to obtain provision of a public service; 2) a ban on the receipt of any benefits, loans, grants or

subsidies, and the possible revocation of those already granted; 3) prohibition to advertise goods or services for a period of between three months and two years.

- **Corruption in judicial proceedings (Article 319-ter of the Criminal Code)**

Corruption in judicial proceedings may be committed in relation to Judges or members of an Arbitration Panel empowered to rule in judicial/arbitration proceedings involving the Group (including auxiliary staff and court-appointed experts), and/or representatives of the Public Administration, when the latter is the counterparty in a dispute, in order to illegally obtain favourable judicial and/or extrajudicial decisions.

Fines pursuant to Italian Legislative Decree no. 231/01: from 200 to 600 units paragraph 1), and from 300 to 800 units (paragraph 2).

Bans pursuant to Italian Legislative Decree no. 231/01: 1) a ban on the exercise of the profession; 2) the suspension or revocation of any authorizations, licences or concessions favouring commission of the crime; 3) prohibition to enter into contracts with the Public Administration other than in order to obtain provision of a public service; 4) a ban on the receipt of any benefits, loans, grants or subsidies, and the possible revocation of those already granted; 5) prohibition to advertise goods or services. All for a period of at least one year.

- **Corruption of a person charged with a public service (Article 320 of the Criminal Code.)**

The provisions of Article 319 (Corruption relating to performance of an act contrary to official duties) also apply if the act is committed by a person assigned to a public service; the provisions of Article 318 also apply to a person assigned to a public service if said person acts in his/her capacity as a public employee. In any case, the penalties are reduced by no more than one third.

Fines pursuant to Italian Legislative Decree no. 231/01: the same fines provided for in the case of the crimes under Articles 318 and 319 of the Criminal Code.

Bans pursuant to Italian Legislative Decree no. 231/01: 1) a ban on the exercise of the profession; 2) the suspension or revocation of any authorizations, licences or concessions favouring commission of the offence; 3) prohibition to enter into contracts with the Public Administration other than in order to obtain provision of a public service; 4) a ban on the receipt of any benefits, loans, grants or subsidies, and the possible revocation of those already granted; 5) prohibition to advertise goods or services. All for a period of at least one year.

- **Penalties for the corrupter (Article 321 of the Criminal Code)**

"The penalties established in paragraph one of Article 318, in Article 319, in Article 319-bis, in Article 319-ter and in Article 320 in relation to the aforementioned hypotheses of Articles 318 and 319, also apply to any person who gives or promises to give a public official or a person charged with a public service money or benefits in kind."

Fines pursuant to Italian Legislative Decree no. 231/01: in the case of offences under Article 381 of the Code of Criminal Procedure, from 100 to 200 units; in the case of crimes under Articles 319 and 319-ter of the Criminal Code, from 200 to 600 units. In the case of crimes under Articles 319-bis and 319-ter paragraph 2 of the Criminal Code, between 300 and 800 units.

Bans pursuant to Italian Legislative Decree no. 231/01: not provided for.

- **Unlawful inducement to give or promise benefits (Article 319-quater of the Criminal Code)**

Italian Law No. 190 of 6 November 2012 ("Provisions for the prevention and suppression of corruption and illegality in the public administration", or the so-called "Severino Law") introduced a new offence prosecutable under Article 319-*quater* of the Criminal Code (Unlawful inducement to give or promise benefits).

The principal novelties vis-à-vis Italian Legislative Decree no. 231/01 consist in the introduction of the following new offences:

Article 319-*quater* of the Italian Criminal Code, *"Unlawful inducement to give or promise benefits": 1) Except where the act constitutes a more serious*

offence, a Public Official or public service officer who, abusing of his title or powers, induces someone into unduly giving or promising, to himself or to a third party, money or other benefit, shall be punished with imprisonment of between six and ten-and-a-half years. 2) in those cases provided for by the first paragraph, any person who gives or promises money or benefits in kind shall be punished with imprisonment of up to three years".

The penalty provided for ranges between 300 and 800 units (the equivalent of a fine of up to one million two hundred thousand euro), together with the possible disqualification from office for a period of at least one year.

- **Inducement to corruption (Article 322 of the Criminal Code)**

"Whoever offers or promises money or any other undue benefit to a public official or a public employee charged with a public service, in order to induce them to perform an official act or service, shall be subject, whenever the offer or promise is not accepted, to the punishment prescribed in the first paragraph of Article 318, reduced by one third.

If the offer or promise was made in order to induce a public official or person charged with a public service to omit o delay an official act or service, or to commit an act contrary to their duties, the offender shall be subject, if the offer or promise was not accepted, to the punishment prescribed in Article 319, reduced by one-third.

The punishment provided for in the first paragraph shall apply to a public official or a public employee charged with a public service who solicits the promise, or the giving, of a sum of money, or other benefits from a private individual for the purposes indicated in Article 318.

The punishment provided for in the second paragraph shall apply to a public official or a public employee charged with a public service who solicits the promise, or the giving, of a sum of money, or other benefits from a private individual for the purposes indicated in Article 319."

Fines pursuant to Italian Legislative Decree no. 231/01: in the case of offences under Article 381 of the Code of Criminal Procedure, from 100 to 200 units; in

the case of offences under Articles 319 and 319-ter of the Criminal Code, from 200 to 600 units. In the case of offences under Articles 319-bis and 319-ter, paragraph 2, of the Criminal Code, between 300 and 800 units.
No bans are provided for.

- **Fraud (Article 640 of the Criminal Code)**

"Anyone who, by misleading someone by artifice or deception, obtains to the detriment of others an unjust profit for themselves or others, shall be liable to a term of imprisonment of between six months and three years and a fine of between €51 and €1,032. The penalty shall be imprisonment of between one and five years and a fine of €309 to €1,549: 1) if the offence is committed to the detriment of the State or another Public Entity, or on the pretext of exonerating someone from military service; 2) if the offence is committed by inducing in the victim the fear of an imaginary danger or the erroneous belief of being required to carry out the order of an Authority. The offence is prosecutable in response to the filing of a complaint by the victim, unless any of the circumstances envisaged in the previous point or other aggravating circumstances, arise."

Fines pursuant to Italian Legislative Decree no. 231/01: between 100 and 500 units, increased by between 200 and 600 units in the event that the Entity has made a significant profit or that serious damage has been caused.
Bans pursuant to Italian Legislative Decree no. 231/01: 1) prohibition to enter into contracts with the Public Administration other than in order to obtain provision of a public service; 2) a ban on the receipt of any benefits, loans, grants or subsidies, and the possible revocation of those already granted; 3) prohibition to advertise goods or services: All for a period of between three months and two years.

- **Aggravated fraud with intent to obtain public funds (Article 640-bis of the Criminal Code)**

"The penalty shall be imprisonment of between one and six years and shall be automatically subject to prosecution if the act indicated in Article 640 concerns

subsidies, grants, financing, preferential financing or other funding of the same type, howsoever named, granted or disbursed by the State, by other public entities, or by the European Communities."

Fines pursuant to Italian Legislative Decree no. 231/01: between 100 and 500 units, increased by between 200 and 600 units in the event that the Entity has made a significant profit or that serious damage has been caused.

Bans pursuant to Italian Legislative Decree no. 231/01: 1) prohibition to enter into contracts with the Public Administration other than in order to obtain provision of a public service; 2) a ban on the receipt of any benefits, loans, grants or subsidies, and the possible revocation of those already granted; 3) prohibition to advertise goods or services: All for a period of between three months and two years.

- **Computer fraud against the State or another Public Entity (Article 640-ter of the Criminal Code)**

""Anyone who, by altering in any way the operation of a computer or communications system or by unduly interfering in any manner with data, information or programs contained in or pertaining to a computer or communications system, obtains for themselves or for others an unfair benefit to the detriment of others, shall be liable to a term of imprisonment of between six months and three years and a fine of between €51 and €1,032.

The term of imprisonment shall be of between one and five years and a fine of between €309 and €1,549 if one of the circumstances provided for at number 1), second paragraph, of Article 640, arises, i.e. if the act is committed by abuse of the position of system operator.

The offence is prosecutable upon the filing of a complaint by the injured party, except where any of the circumstances indicated in the second paragraph, or another aggravating circumstance, arise."

Fines pursuant to Italian Legislative Decree no. 231/01: between 100 and 500 units, increased by between 200 and 600 units in the event that the Entity has made a significant profit or that serious damage has been caused.

Bans pursuant to Italian Legislative Decree no. 231/01: 1) prohibition to enter into contracts with the Public Administration other than in order to obtain provision of a public service; 2) a ban on the receipt of any benefits, loans, grants or subsidies, and the possible revocation of those already granted; 3) prohibition to advertise goods or services: All for a period of between three months and two years.

2 Areas at risk of crime

The potential risk areas that Banca Sistema has identified in its relations with the Public Administration, and within the context of the offences as per the Decree, are those pertaining to:

a. the acquisition without recourse of receivables payable by the Public Administration and the consequent relations with the latter in regard to the monitoring and collection of the transferred receivables;
b. the negotiation, conclusion and performance of contracts/agreements with the Public Administration (including settlement agreements regarding the acquired receivables referred to in point a) above, through negotiated procedures (direct assignment or private negotiation) or through public tenders (open or limited);
c. the management of relations with the Public Administration – including Public Supervisory Authorities (the Bank of Italy, CONSOB, the Financial Information Unit, Ministries, the Personal Data Protection Authority) that operate as public authorities with regard to certain areas of responsibility;
d. the management of relations with the Public Administration for the purpose of obtaining permissions/licences/authorizations;
e. relations with the investigating authorities (Carabinieri, Italian State Police, Municipal Police, Financial Police);
f. the management of the software programmes of Public Entities (Local Health Authorities) or those provided by third parties on behalf of Public Entities, and telecommunications connections, or the transmission of data on computerized media, to Public Entities;
g. relations with agents, financial agents, credit brokers, introducers, financial promoters and brokers (the selection, creation and regulation of the relationship, the calculation of fees, the management and termination of the relationship) who in turn deal with the Public Administration;
h. the preparation of tax returns or withholding tax returns, or any other declarations pertaining to the payment of taxes in general;
i. the management of free gifts/complimentary items/advertising;

j. the management of personnel hiring procedures and of relations with Public Entities regarding the hiring of personnel belonging to protected categories of workers, or whose hiring is subject to preferential treatment;
k. the management of relations with Public Entities as regards occupational health and safety (pursuant to Italian Legislative Decree no. 81/08);
l. the management of personnel's social security contributions and/or the management of the corresponding audits/inspections;
m. verification of the settlement of employees' expenses;
n. pawn credit.

Any amendments or additions to the aforementioned risk areas shall be the responsibility of the Board of Directors, also upon proposal from the Supervisory Body.

3 Rules of Conduct

The control system

In the performance of their duties/functions, as well as being aware of, and complying with, the rules laid out in the Bank's Articles of Association, operating procedures and all other internal rules pertaining to the system of Corporate Governance, the Recipients must also comply with the rules of conduct set out in this Model.

More specifically, this Special Part expressly bans:

1. any conduct constituting the types of offence mentioned above (Articles 24 and 25 of the Decree), or any conduct which although in itself does not constitute any type of offence, may potentially constitute one of the offences in question;
2. the provision of services to suppliers, consultants, partners and co-workers in general, which are not duly justified within the context of the contractual relationship with such parties, or in relation to the type of assignment to be performed and to local practices;

3. the proposal of any commercial opportunities that may personally benefit employees of the Public Administration, or the agreement of other benefits of any kind (the promise of hiring, etc.) to the advantage of representatives of the Public Administration, or to any other persons related to the latter;
4. the offering of any money or gifts to public officials, or the receipt of such, beyond generally accepted practice. More specifically, no form of gift may be made to any Italian or foreign public officials or their families, that may affect their discretionary powers or independent judgment, or may result in the company obtaining any advantage. Permitted free gifts are always characterized by their extremely limited value, or by the fact that they are designed exclusively to promote the Bank's image. The SB shall be exhaustively informed of all gifts offered – except for those of limited value – so as to be able to carry out the adequate checks;
5. the disclosure of untrue information to the Public Administration, the preparation and supply of false documents, and the omission of due information;
6. the violation of the Public Administration's computer systems in order to obtain or manipulate information to the Bank's advantage;
7. the conclusion of contracts without the necessary powers to do so. Any person who has relations, or negotiates, with the Public Administration, may not conclude any contracts he/she has negotiated if he/she does not possess the specific powers required to do so: contracts may only be negotiated and concluded based on an official power of attorney or authorization to such end, bearing details of any restrictions and liabilities;
8. the use of artifice and deception to mislead the Public Administration and induce it into wrongly evaluating the technical and economic characteristics of those products or services offered or supplied, or of valuable consideration in general;
9. the misappropriation, even if only partial, of grants, subsidies and public funding from the purposes for which were obtained;

10. the making of any payments in cash, unless express authorization for such has been granted by the Finance Department, which may only grant such in those cases in which it is specifically required by the regulations governing the Public Entity's activities, and in any case subject to the recording of such payments under the corresponding financial statement items ;
11. any false representations to national or EC public bodies in order to obtain public funding, grants or subsidized loans, or the untruthful recording of the operations for which public funds have already been disbursed;
12. access to financial resources:
    a. spending must only be carried out on the basis of an official proxy , authorization or power of attorney detailing spending limits, restrictions and liability;
    b. spending must only be carried out on the basis of documents justifying such, complete with the grounds for the spending, and certification of the pertinence and congruence of costs, duly approved by senior management and stored;
13. the assignment of contracts for advisory, brokerage and similar services, in the absence of the corresponding powers. Nobody alone may freely appoint consultants, brokers or other persons providing similar professional services:
    a. the appointment may only be made on the basis of an official proxy , authorization or power of attorney detailing spending limits, restrictions and liability;
    b. the appointment shall be made on the basis of a list of suppliers/consultants/professionals, managed by the competent department. Inclusion on/elimination from the list shall be based on objective criteria. Reasons shall be given for the identification of the person(s) to be appointed, and this shall be duly documented;
    c. appointments may only be made on the basis of justifying documents detailing the grounds for any appointment and the names of those

appointed, and certification of the pertinence and congruence of such appointments, duly approved by senior management and stored.

In order to prevent the aforementioned forms of conduct:

- there must be a clear separation of roles and responsibilities, that is, a clear distribution of duties among the various functions, and thus between who prepares and who signs the documents to be submitted to the Public Administration (for example, in the case of a contract concluded with a Local Health Authority, there must be a very clear separation of duties, within the Bank, between (i) who proposes the conclusion of the contract; (ii) who carries out the risk assessment in order to see whether the contract may be concluded or not; (iii) who gathers and arranges the necessary documents; and (iv) who approves and signs the contract);
- working agreement with partners must be made in writing, and must detail all the terms and conditions of the agreement itself, in particular with regard to the financial conditions agreed for joint involvement in the procedure, and must be proposed, verified and approved by at least two people belonging to the Bank;
- no form of payment in cash or in kind may be made beyond the limits established by the Bank;
- those who control and monitor compliance in terms of performance of the aforementioned activities must pay particular attention to the implementation of the formalities and must report any irregularities to the SB;
- any critical issues or conflicts of interest that arise within the context of relations with the Public Administration, must be reported to the SB in a written note;
- with regard to the management of relations with the financial administration, the following must be done:

a. the procedures governing attendance at any legal, tax, administrative and/or supervisory inspections or audits, and the

management of relations with Public Entities for the purpose of obtaining authorizations, licences or anything else, must be duly registered;

b. a record must be kept, through the drafting of specific reports, of the entire inspection procedure. Should the final report indicate any critical issues, the SB must be informed of such in writing, by the person in charge of the function involved.

Agreements with contractors

Any agreements with contractors who have dealings with the Public Administration, must contain a clause governing the consequences of said contractors' failure to fulfil their obligations under the Decree and the ethical principles established by the Model.

4 The Supervisory Body's duties

Without prejudice to the Supervisory Body's discretionary power to carry out specific controls following reports received (see the provisions of the General Part of this Model), it is the Supervisory Body's duty to:

a. carry out regular controls regarding compliance with this Special Part, and to evaluate its effectiveness in preventing the commission of those offences set out in Sections 24 and 25 of the Decree, through random checks on the aforementioned risk areas;
b. regularly check – with the support of the appointed departments – the system of proxies and powers of attorney in force, and recommend any amendments to such should the management power and/or the qualification do not correspond to the representative powers assigned to company representatives;
c. examine any specific reports received from control bodies or from third parties, evaluate the reliability of such, and carry out those inspections deemed necessary or appropriate;
d. report any breach of the Model to the appointed bodies, according to the disciplinary system for the adoption of punitive measures;
e. update the Model, informing the Board of Directors of any appropriate additions that could be made, together with the measures deemed necessary in order to maintain the Model's adequacy and/or effectiveness.

B) CORPORATE CRIMES

1 Corporate crimes

The following corporate crimes may give rise to an Entity's corporate liability under Section 25-*ter*[5] of Italian Legislative Decree no. 231/2001:

- **False corporate disclosure (Article 2621 of the Italian Civil Code6)**

"Save as otherwise provided in Article 2622, the directors, general managers, executive managers appointed to draft the company's financial statements, auditors and liquidators who, with the intention of deceiving the shareholders or the public and with the aim of securing for themselves or others an unjust profit, make statements of substantive facts which are untrue in the company's financial statements, reports or other company documents provided for by law which are intended for the shareholders or for the public, or who omit information, the communication of which is required by law, concerning the financial position, assets and liabilities of the company or the group to which that company belongs, so as to give the recipients a false impression of that position, shall be liable to imprisonment for a term of between one year and five years. The same punishment also applies if the false disclosures or omissions regard assets possessed or managed by the company on behalf of third parties".

Fines pursuant to Italian Legislative Decree no. 231/01: from 200 to 400 units; no bans are provided for.

- **False corporate disclosure by listed companies (Article 2622 of the Italian Civil Code7)**

"The directors, general managers, executive managers appointed to draft the company's financial statements, auditors and liquidators of companies issuing financial instruments admitted to trading in a regulated market in Italy or in

[5] Article added by Section 3 of Italian Legislative Decree no. 61 of 11 April 2002.
[6] Article substituted by Italian Law no. 69 of 27 May 2015.

another EU member state, who, with the intention of deceiving the shareholders or the public and with the aim of securing for themselves or others an unjust profit, make statements of substantive facts which are untrue in the company's financial statements, reports or other company documents provided for by law which are intended for the shareholders or for the public, or who omit information, the communication of which is required by law, concerning the financial position, assets and liabilities of the company or the group to which that company belongs, so as to give the recipients a false impression of that position, shall be liable to imprisonment for a term of between three and eight years. The following are equated to those companies indicated in the previous paragraph:

1) companies issuing financial instruments for which an application has been submitted for their admission to trading in a regulated market in Italy or in another EU member state;

2) companies issuing financial instruments that are admitted to trading in an Italian multilateral trading system;

3) companies controlling other companies admitted to trading in a regulated market in Italy or in another EU member state;

4) companies soliciting or managing public savings.

The provisions set out in the foregoing paragraphs shall also apply if the false disclosures or omissions regard assets possessed or managed by the company on behalf of third parties".

Fines pursuant to Italian Legislative Decree no. 231/01: for the 1st paragraph, from 400 to 600 units, and for the 3rd paragraph, from 400 to 800 units; no bans are provided for.

- **Obstruction of supervisory activities (Article 2625 , paragraph 2, of the Italian Civil Code)**

"Directors who, by concealing documents or by other deceptive means, impede or obstruct the supervisory activities that shareholders, other corporate bodies or the independent auditors are legally obliged to perform, shall be liable to an administrative fine of up to €10,329. If such conduct has caused damage to the

[7] See Note 5.

shareholders, a term of imprisonment of up to one year may be imposed, following a complaint by the injured party. The term of imprisonment is doubled if the offence involves companies listed on Italian regulated markets or those of other member states of the European Union, or companies in which the public hold a significant shareholding, as defined in Section 116 of the Consolidated Law contained in Italian Legislative Decree no. 58 of 24 February 1998."

Fines pursuant to Italian Legislative Decree no. 231/01: from 200 to 360 units; no bans are provided for.

- **Unlawful return of capital contributions (Article 2626 of the Italian Civil Code)**

"Directors who, except in cases of a lawful reduction of share capital, return, even fictitiously, contributions to shareholders or absolve them of the obligation to make such contributions, shall be liable to a term of imprisonment of up to one year."

Fines pursuant to Italian Legislative Decree no. 231/01: from 200 to 360 units; no bans are provided for.

- **Unlawful distribution of profits and reserves (Article 2627 of the Italian Civil Code)**

"Unless the act constitutes a more serious offence, directors who distribute profits or advances on profits which were not actually earned or destined by law to the reserve, or that distribute reserves, including those which do not consist of profits and which cannot by law be distributed, shall be liable to a term of imprisonment of up to a year. The return of the profits or the reconstitution of the reserves before the deadline for approval of the financial statements extinguishes the offence."

Fines pursuant to Italian Legislative Decree no. 231/01: from 200 to 260 units; no bans are provided for.

- **Unlawful transactions in shares of the company or its parent company (Article 2628 of the Italian Civil Code)**

"Directors who, except in the cases permitted by law, purchase or subscribe company shares or quotas, thereby damaging the integrity of the share capital or the reserves that by law cannot be distributed, shall be liable to a term of imprisonment of up to a year. The same term of imprisonment shall apply to directors who, except in the cases permitted by law, purchase or subscribe shares or quotas issued by the parent company, causing damage to the share capital or the reserves that by law cannot be distributed. If the share capital or the reserves are reconstituted before the deadline for the approval of the financial statements for the financial year in which the criminal conduct took place, the offence is extinguished."

Fines pursuant to Italian Legislative Decree no. 231/01: from 200 to 360 units; no bans are provided for.

- **Transactions to the detriment of creditors (Article 2629 of the Italian Civil Code)**

"Directors who, in violation of the provisions of law regarding the protection of creditors, carry out reductions in the share capital or mergers or demergers with other companies, which cause damage to creditors, shall be liable, upon the complaint of an injured party, to a term of imprisonment of between six months and three years. The payment of compensation for the damage to creditors before legal proceedings commence extinguishes the offence".

Fines pursuant to Italian Legislative Decree no. 231/01: from 300 to 660 units; no bans are provided for.

- **Failure to disclose a conflict of interest (Article 2629-bis of the Italian Civil Code)**

"A director or member of the management board of a company listed on Italian regulated markets or those of other member states of the European Union, or of companies in which the public hold a significant shareholding, pursuant to Section 116 of the Consolidated Law on Finance, or a person subject to supervision pursuant to the Consolidated Law on Banking, to the aforementioned

Consolidated Law on Finance, to Italian Legislative Decree no. 209 of 7 September 2005, or to Italian Legislative Decree no. 124 of 21 April 1993, who violates the obligations established in Article 2391, first paragraph, shall be liable to a term of imprisonment of between one and three years, if the violation gives rise to damage to the company or to third parties."

Fines pursuant to Italian Legislative Decree no. 231/01: from 400 to 1,000 units; no bans are provided for.

- **Fraudulent formation of capital (Article 2632 of the Italian Civil Code)**

"*Directors and shareholders who, even partly, fraudulently form or increase the share capital by the allocation of shares or quotas to an extent that as a whole is greater than the amount of the share capital, or reciprocally subscribe shares or quotas, or significantly overestimate contributions in kind, receivables or the assets of the company in the event of transformation, shall be liable to a term of imprisonment of up to one year*".

Fines pursuant to Italian Legislative Decree no. 231/01: from 200 to 360 units; no bans are provided for.

- **Improper distribution of company assets by liquidators (Article 2633 of the Italian Civil Code)**

"*Liquidators who, by distributing company assets among shareholders before paying creditors of the company or setting aside the funds necessary to satisfy the claims of creditors, thereby causing damage to creditors, shall be liable, upon the complaint of the injured party, to a term of imprisonment of between six months and three years. The payment of compensation for the damage to creditors before legal proceedings commence extinguishes the offence*".

Fines pursuant to Italian Legislative Decree no. 231/01: from 300 to 360 units; no bans are provided for.

- **Corruption between private individuals (Article 2635 of the Italian Civil Code)**

"1. Unless the fact constitutes a more serious offense, the directors, the general managers, the managers in charge of drafting the corporate accounting documents, the statutory auditors and the liquidators, who, following the giving or the promise of money or other benefits, for themselves or for others, perform or omit acts, in violation of the obligations inherent in their office or fidelity obligations, causing harm to society, are punished with imprisonment from one to three years.

2. The sentence of imprisonment up to one year and six months shall apply if the fact is committed by those subject to the management or supervision of one of the persons referred to in the first paragraph.

3. Whoever gives or promises money or other benefits to the persons indicated in the first and second paragraphs shall be punished with the penalties provided for therein.

4. The penalties established in the previous paragraphs are doubled if the crimes are committed by companies with securities listed on regulated markets in Italy or in other European Union countries or that are widely distributed among the public pursuant to Article 116 of the Consolidated Law on the provisions financial intermediation, pursuant to Legislative Decree 24 February 1998, n. 58, and subsequent modifications.

5. The complaint is filed by the injured party, except that it results in a distortion of competition in the acquisition of goods or services".

The Entity is responsible if one of the Recipients carries out the conduct described by the third paragraph of the rule: in other words, only the entity in which the corrupter operates is punished.

Pecuniary sanctions pursuant to Legislative Decree No. 231/01: From 400 to 600 quotas, increased from 600 to 900 quotas if the institution has achieved a significant profit.

Disqualification sanctions pursuant to Legislative Decree 231/01: 1) interdiction from the exercise of the activity; 2) suspension or revocation of authorizations, licenses or concessions functional to the commission of the offense; 3) prohibition of contracting with the Public Administration, except to obtain the services of a public service; 4)

exclusion from subsidies, loans, grants or subsidies and the possible revocation of those already granted; 5) prohibition to advertise goods or services. For a maximum period of two years.

- **Instigation of corruption among private individuals Istigazione alla corruzione tra privati (Article 2635-bis of the Italian Civil Code)**

"1. Anyone who offers or promises money or other benefits not due to directors, general managers, managers in charge of drafting corporate accounting documents, statutory auditors and liquidators, companies or private entities, and 'those who work in them with the exercise of managerial functions, so that 'performs or omits a deed in violation of the obligations inherent in their office or fidelity obligations, subject, if the offer or promise is not accepted, to the penalty established in the first paragraph of' Article 2635, reduced by one third.

2. The penalty referred to in the first paragraph applies to directors, general managers, managers in charge of drafting corporate accounting documents, statutory auditors and liquidators, companies or private entities, as well as' those who work in them with the exercise of managerial functions, which solicit for themselves or others, even through a third party, a promise or donation of money or other benefits, to perform or to omit an act in violation of the obligations inherent to their office or fidelity obligations , if the solicitation is not accepted".

Pecuniary sanctions pursuant to Legislative Decree no. 231/01: From 200 to 400 quotas, increased from 300 to 600 quotas if the institution has achieved a significant profit.

Disqualification sanctions pursuant to Legislative Decree 231/01: 1) interdiction from the exercise of the activity; 2) suspension or revocation of authorizations, licenses or concessions functional to the commission of the offense; 3) prohibition of contracting with the public administration, except to obtain the services of a public service; 4) exclusion from subsidies, loans, grants or subsidies and the possible revocation of those already granted; 5) prohibition to advertise goods or services. For a maximum period of two years.

- **Unlawful influence over the Shareholders' Meeting (Article 2636 of the Italian Civil Code)**

"*Anyone who, by false or fraudulent acts, procures a majority at a Shareholders' Meeting in order to obtain an unjust profit for themselves or others, shall be liable to a term of imprisonment of between six months and three years*".

Fines pursuant to Italian Legislative Decree no. 231/01: from 300 to 660 units; no bans are provided for.

- **Market rigging (Article 2637 of the Italian Civil Code)**

"*Anyone who provides false information, carries out fictitious transactions, or by other artifice effectively causes a significant alteration in the price of financial instruments which are not listed or for which no application for admission to trading on a regulated market has been submitted, or who significantly affects the trust that the public places in the financial stability of banks or banking groups, shall be liable to a term of imprisonment of between one and five years."*

Fines pursuant to Italian Legislative Decree no. 231/01: from 400 to 1,000 units; no bans are provided for.

- **Obstruction of the activities of public supervisory authorities (Article 2638 of the Italian Civil Code)**

This offence is committed by anyone who reports material facts, in the mandatory reports to the supervisory authorities, that do not conform to the truth even if subject to valuation, on the financial and asset position of entities subject to supervision, with the intent of obstructing the activities of said authorities, or who, with the same intent, conceals by other fraudulent means, in whole or in part, facts which should have been reported concerning the said situation.

Fines pursuant to Italian Legislative Decree no. 231/01: from 400 to 800 units; no bans are provided for.

2 Areas at risk from the commission of offences

The areas that Banca Sistema has identified as being potentially at risk from the commission of corporate crimes are those pertaining to:

a. the handling of confidential information;
b. the fulfilment of disclosure obligations regarding potential conflicts of interest;
c. the drafting of financial statements, reports and other corporate communications provided for by law;
d. the management of shareholdings, of share capital transactions and of extraordinary transactions;
e. the preparation and holding of Shareholders' Meetings, as well as the keeping of minutes thereof, meetings of the Board of Directors and of the Executive Committee (if established);
f. the handling of relations with the Board of Statutory Auditors, independent auditors and other corporate bodies;
g. the reporting to the Supervisory Authorities, and the handling of relations with such;
h. the management of judicial and extra-judicial disputes, as well as out-of-court settlements;
i. the selection and hiring of personnel;
j. the management of free gifts, expenses, charitable actions and sponsorships;
k. the handling of the reimbursement of expenses.
l. pawn credit.

Any changes or additions to the aforementioned risk areas shall be the responsibility of the Board of Directors, also upon proposal from the SB.

3 Rules of Conduct

In the performance of their duties/functions, as well as being aware of, and complying with, the rules laid out in the Bank's Bye-laws, operating procedures and all other internal rules pertaining to the system of Corporate Governance, the Recipients must also comply with the rules of conduct set out in this Model.

More specifically, this Special Part expressly prohibits the engaging in any form of conduct that may give rise to one of the aforementioned criminal offences (pursuant to Section 25-ter of the Decree), or in any form of conduct which although in itself does not constitute an offence, may in theory give rise to the commission of one of the offences in question.

Consequently, this Special Part establishes the obligation, on the Recipients' part, to:

a. behave in a manner that is fair, transparent, cooperative and respectful of the law and of any internal Company procedures in all acts carried out in the process of drawing up financial statements and other corporate communications, designed to provide shareholders and third parties with fair and correct information about the Company's operating performance, financial position and financial performance. In this regard, the Recipients are specifically forbidden to:
   - prepare or disclose data that are false, incomplete or otherwise not reflective of the truth with regard to the operating performance, financial position and financial performance of the Bank;
   - omit data and information about the operating performance, financial position and financial performance of the Bank, the disclosure of which is required by law;

b. comply with the principles and rules laid out in the instructions for the drafting of the financial statements and of the regular reports governed by law;

c. comply with all statutory provisions that protect the integrity and truthful representation of the amount of the Bank's share capital, so as not to undermine guarantees provided to creditors and other third parties;

d. pursue the corporate interest when managing and carrying out the Bank's activities, up until any winding up or closing down of the Bank itself;
e. ensure that the Bank and its governance bodies function normally, ensuring and facilitating any type of internal control of the Bank's operations that the law may require and encouraging the Shareholders' Meeting to express its will freely;
f. promptly, fairly and in good faith provide all of the communications required by law, and create no obstacle that could prevent the Supervisory Authorities from exercising their powers. It is specifically forbidden to:
    - fail to provide, in a sufficiently complete, clear and prompt manner, all the regular communications required by the applicable laws and regulations;
    - include in the abovementioned communications or transmissions false information, or hide facts that are significant with regard to the Bank's operating performance, financial position and financial performance;
    - engage in conduct that in any way hinders the Administrative Authorities in the performance of their supervisory and inspection functions (e.g., outright opposition, refusal based on a pretext, or simple obstructive behaviour or lack of collaboration, such as delays in publishing communications or in making documents available);
g. formulate specific procedures for the preparation of the financial statements and the management of financial resources;
h. observe the rules governing the correct formation of the price of the financial instruments, and avoid any form of conduct that may significantly alter said price in relation to the current market situation;
i. behave in a correct, truthful manner in relations with the press, the media and financial analysts;
j. refrain from engaging in any conduct that could constitute market abuse;
k. refrain from engaging in fictitious or otherwise fraudulent transactions or disseminating false or incorrect information, for the purpose of causing significant changes in the prices of financial instruments.

In regard to the risk areas identified in this Special Part, the following specific principles of conduct shall be observed, in compliance with the Decree.

More specifically, the annual financial statements, the reports and the other corporate communications provided for by law (presentation of data, the processing and approval thereof) must be drawn up in accordance with specific company procedures that:

- clearly define the data and information that each department is required to provide, the criteria that must be followed when processing these data (for example, the criteria to be followed when evaluating those items on the financial statements that are of an estimated nature, such as receivables and their presumed realizable value, the provision for risks and charges, dividends, the provision for taxes and duties, etc.), and the deadlines for delivery to the appropriate departments;
- require that the data and information be transmitted to the appropriate department by means of a system (including computer systems) that allows the tracing of individual entries and the identification of the parties entering data into the system;
- utilize forecast information shared by the departments involved, and approved by the governing bodies.

Furthermore, communications to shareholders regarding the Bank's operating performance, financial position and financial performance, must be prepared in such a way that the following are indicated clearly and in full:

- the data and information that each department is to provide;
- the accounting principles followed for the processing of the data;
- the deadline for the delivery of said data and information to the appropriate corporate areas.

Finally, in addition to the aforementioned measures and to those already adopted by the Bank, it is hereby established that:

a. provision be made for the holding of at least one Board of Directors meeting each quarter, for the purpose of sharing relevant information pertaining to the management of the Bank;

b. all documents pertaining to the items on the agendas of the Shareholders' Meetings or of the Board of Directors' meetings, or in regard to which the Directors and the Board of Statutory Auditors are required by law to express an opinion, shall be transmitted to said Directors and Statutory Auditors;
c. provision be made for regular meetings to be held between the Board of Statutory Auditors and the Supervisory Body, for the purpose of verifying compliance with provisions pertaining to corporate rules and Corporate Governance.

Any agreements with contractors must contain a clause governing the non-fulfilment by said contractors of their obligations under the Decree, and of the principles established by the Model.

4 The Supervisory Body's duties

Without prejudice to the Supervisory Body's discretionary powers, to be implemented through specific controls following reports received (for details, see the General Part of this Model),the Supervisory Body shall be responsible for:

a. verifying, through random checks on those areas at risk from the commission of offences, the implementation and adequacy of this Model and the due performance of the operations pertaining to the risk areas in relation to the rules set out in this Model (the existence and adequacy of the corresponding power of attorney, spending limits, disclosure to the appointed bodies, etc.);
b. monitoring the effectiveness of any internal procedures for the prevention of the offences referred to in this Special Part;
c. examining any specific reports received from corporate bodies, third parties or company representatives, and carrying out any checks deemed necessary or appropriate in relation to such reports;
d. notifying the appointed authorities of any breach of the Model, on the basis of the disciplinary system for the adoption of punitive measures;
e. updating the Model, by informing the Board of Directors of any appropriate additions to be made, and the measures deemed necessary in order to preserve the adequacy and/or the effectiveness of the Model itself.

C) MARKET ABUSE

1 Market abuse

This Section of the Special Part of the Model was introduced following the listing of Banca Sistema SpA on the STAR market operated by Borsa Italiana SpA, in July 2015.

The offences set out in Section 25-sexies[8] of Italian Legislative Decree no. 231/2001 are the following:

- **Misuse of inside information[9] (Section 184 of Italian Legislative Decree no. 58/1998)**

  1. "This offence, which is punishable with imprisonment for a term of between one and six years, and a fine of between twenty thousand and three million euro, is committed by anyone who, being in possession of inside information obtained as a result of his/her membership of the governing, management or control bodies of a company that issues financial instruments, or of his/her shareholding in the company, or during the exercise of his/her duties, profession, role or office, whether public or not:
     a) buys or sells financial instruments or undertakes other transactions on them, directly or indirectly, on his/her own account or on behalf of third parties, using the inside information acquired by the above means;
     b) communicates such information to another person, other than in the exercise of his/her normal duties, profession, role or office;
     c) advises or induces others, based on the inside information in his/her possession, to execute transactions listed under letter a) above.
  2. The offence of misuse of inside information as per point 1 above, is also committed by anyone who, being in possession of inside information

[8] Section added by Italian Law no. 62, Section 9, of 18 April 2005.

[9] Pursuant to Section 181 of the Consolidated Finance Act, "inside information" means information of a specific nature that has not been made public and that concerns, directly or indirectly, one or more issuers of financial instruments, or one or more financial instruments, which if it were made public, could significantly affect the prices of such instruments, or the prices of any related financial derivatives (so-called *price sensitive* derivatives).

obtained while planning or committing an offence, undertakes one of the actions referred to in point 1, and shall be punished accordingly.

3. The court may increase the fine by up to three times, or to the greater sum of ten times the product or the profit gained as a result of the offence, if, due to the significantly abusive nature of the conduct, to the personal characteristics of the guilty party, or to the entity of the product or profit gained as a result of the offence, said fine appears inadequate even if applied to the full.
4. For the purposes of this Article, financial instruments shall also include those financial instruments referred to in Article 1, paragraph 2, the value of which depends on a financial instrument as per Section 180, paragraph 1, letter a)".

- **Market manipulation10 (art. 185 of Legislative Decree no. 58/1998)**

"1. This offence is committed by anyone who spreads false information or carries out fake transactions or other acts of deception directly aimed at causing a considerable change in the price of financial instruments, and is punishable with imprisonment for a term of between one and six years, and a fine of between € 20,000.00 and € 5,000,000.00.

2. The court may increase the fine by up to three times, or to the greater sum of ten times the product or the profit gained as a result of the offence, if, due to the significantly abusive nature of the conduct, to the personal characteristics of the guilty party, or to the entity of the product or profit gained as a result of the offence, said fine appears inadequate even if applied to the full.

2-bis. In case of transactions concerning those financial instruments referred to in Section 180, paragraph 1, letter a), number 2), the penalty is a fine of up to € 103,291.00 and imprisonment for a term of up to three years".

In both of the above cases, no bans are provided for. It should also be pointed out that Sections 187-*bis* and 187-*ter* of the Consolidated Finance Act

[10] The legal assets that the rule is designed to safeguard are the integrity of regulated financial markets, and the protection and growth of investors' trust.

(introduced by EU law) standardize the administrative offences of misuse of inside information and of market manipulation. These latter offences are punishable - subject to the corresponding criminal penalties that apply when the offence constitutes a criminal offence – with administrative fines. It should be noted that, insofar as they are administrative offences, the penalties provided for by the Consolidated Law on Finance shall apply even when the aforesaid forms of conduct are the result of mere negligence. The power to inflict such administrative penalties is given to the CONSOB by Section 187-*bis*.

The administrative penalty system is completed by Section 187-quinquies of the Consolidated Law on Finance, which establishes that the CONSOB may apply fines ranging from 100,000 to 15 million euro, or from 100,000 to 25 million euro, for the misuse of inside information and for market manipulation, respectively, and such fines may be increased to ten times the product or profit made by the entity following commission of the offence, if the product or profit is substantial.

Thus if the alleged offence is of a criminal nature, any liability on the part of the entity shall be ascertained by the court; if, on the other hand, the offence in question is of an administrative nature, committed by anyone in the interests or to the benefit of the entity – then the due verification and sanctioning of such shall be carried out by the CONSOB. In this regard, the Consolidated Law on Finance establishes the relationship between administrative and criminal proceedings (Chapter V, Sections 187-*decies* ff.), and with regard to the various aspects of verification of the liability of those involved, it establishes that "*the administrative proceedings and appeal proceedings referred to in Section 187-septies, may not be suspended due to the pending criminal proceedings regarding the same facts, or regarding facts the verification of which are decisive for the settlement of said proceedings*".

Thus the same case/news of a wrongdoing could be, at one and the same time, the subject-matter of criminal proceedings before a trial court and of administrative proceedings before the CONSOB, with the consequent verification

of the entity's liability for the very same offence before both the court and the aforesaid authority.

2 Areas at risk of crime

Misuse of inside information

A top manager, or a subordinate, who falls within one of the categories as per Section 184, paragraph 1, of the Consolidated Law on Finance, who utilizes information that he/she has come into possession of, and performs one of the following actions:

- the purchase or sale of financial instruments issued by the company or by a company within the Group, or any other transactions on such instruments, either directly or indirectly;
- the disclosure of information to other persons other than within the context of the performance of ordinary working duties;
- recommending that others, or inducing others to, purchase or sell financial instruments issued by the company or by companies within the Group, or carry out other transactions on such instruments.

The same transactions matter if they are performed by top managers, or by subordinates, who do not fall within one of the categories as per Section 184, paragraph 1, of the Consolidated Law on Finance, but who nevertheless come into possession of inside information when preparing or carrying out criminal activities (Section 184, paragraph 2, of the Consolidated Law on Finance).

With regard to administrative offences only, the same transactions matter even if they are performed by those persons referred to in Section 187-bis, paragraph 4, of the Consolidated Law on Finance.

Thus, the following areas or functions are potentially at risk from the commission of offences:

- Corporate bodies;
- Finance/Treasury Division;
- Investor Relations Area;

- Legal Affairs Division and the Company's Secretary's Office;
- Marketing and Communications Division;
- Other persons included in the registers of persons with access to inside information.

Market manipulation

Fictitious or misleading transactions (Section 187-ter, paragraph 3, letter a), of the Consolidated Law on Finance):

- Wash trades;
- Alteration of the framework of transactions *(painting the tape)*;
- Orders combined inappropriately;
- Entering of orders with no intention of carrying them out.

Therefore, the Finance/Treasury Division is potentially at risk.

Transactions that fix prices at anomalous or artificial levels (Section 187-ter, paragraph 3, letter b), of the Consolidated Law on Finance):

- Marking the close;
- Colluding on the secondary market following a placement within the context of a public offering;
- Abusive squeeze;
- Establishing a price floor;
- Transactions carried out in one market in order to unduly influence the prices of a financial instrument in a related market.

Therefore, the Finance/Treasury Division is potentially at risk.

Transactions involving the use of artifice, deception or other expedients (Section 187-ter, paragraph 3, letter c), of the Consolidated Law on Finance):

- concealing ownership;
- disclosure of false or misleading market information by means of communication, including the Internet, or by any other means;
- pumping and dumping;

- trashing and cashing;
- opening a position and then closing it immediately after it has been made public.

As a result, the following areas/functions are potentially at risk: i) members of corporate bodies; ii) Finance/Treasury Division; Legal/Corporate Affairs Division; iii) Investor Relations Area; iv) Marketing Division.

Disclosure of false or misleading information (Section 187-ter, paragraph 1, of the Consolidated Law on Finance):

This form of market manipulation entails the disclosure of false or misleading information through means of communication, or through other pre-established forms of conduct, not necessarily in the presence of market transactions.

As a result, the following areas/functions are potentially at risk: i) members of corporate bodies; ii) Finance/Treasury Division; Corporate Affairs Area; iii) Investor Relations Area; iv) Marketing Division; Commercial Factoring Division.

3 Rules of conduct

As a rule, and in order to prevent the commission of market abuse offences, Recipients who carry out their activities within the context of the previously-identified areas at risk of commission of offences, and subject to the provisions of the Code of Conduct, are bound to comply with the following general principles of conduct:

a) to refrain from engaging or participating in any conduct that, considered either individually or collectively, could constitute the aforementioned offences;
b) to maintain a conduct based on the principles of correctness, transparency, cooperation and compliance with the provisions of law and of regulations in force, when carrying out all the activities during which they come into possession of inside information, or of information that could enable them to engage in the manipulation of information or of market operations;

c) to comply with the rules governing the correct formation of the prices of financial instruments, and to avoid any conduct that could cause a significant alteration of such prices vis-à-vis the existing market situation;

d) to refrain from acting in concert with one or more persons in order to acquire a position regarding the supply of, or demand for, a financial instrument that has the effect of fixing, directly or indirectly, purchase or selling prices, or of determining other unfair trade conditions;

e) to refrain from engaging in simulated or otherwise fraudulent transactions, and from disseminating false or incorrect information capable of causing a significant alteration in the prices of financial instruments;

f) to behave in a correct, truthful manner in relations with the press, the media and financial analysts;

g) to refrain from trading in a financial instrument in the knowledge of a conflict of interest, unless such conflict is made explicit in the forms provided for by internal regulations.

4 The Supervisory Body's duties

Without prejudice to the duties and functions of the Supervisory Body stipulated in the General Part of this Model, in order to prevent the offences described in this Special Part being committed, the Supervisory Body is bound to:

- verify compliance with, and the implementation and adequacy of, the Model and the rules of corporate governance, in relation to the need to prevent commission of the offences of market manipulation and market abuse;
- monitor the effective application of the Model, and observe any variations in conduct that emerge from the analysis of the information and reports received;
- examine any specific reports received from the control bodies and from any employees, and carry out any checks deemed necessary or appropriate in relation to such reports;

- notify the appointed authorities of any breach of the Model, according to the disciplinary system for the adoption of punitive measures;
- constantly monitor the updating of the Model, and recommend to the appointed corporate bodies in question the measures deemed necessary in order to preserve the adequacy and/or the effectiveness of the Model itself;
- regularly check, with the support of the appointed company bodies, that the system of delegated powers in force is relevant to the Bank's everyday operations;
- verify compliance with the operating procedures and the principles set out therein, with specific regard to transactions on listed and non-listed financial instruments;
- verify any anomalies reported during trading which may reasonably be deemed capable of constituting breaches of the provisions governing the misuse of inside information and market manipulation.

In order to effectively and promptly perform the aforesaid duties, the Supervisory Body must be provided with adequate flows of information also regarding the offences of market manipulation and market abuse, as described in the General Part of this Model.

Furthermore, it should be noted that the Supervisory Body's duties also include the reporting of the results of its monitoring and control activities, with regard to the offences of market manipulation and market abuse, to the Board of Directors and to the Board of Statutory Auditors.

D) MONEY LAUNDERING CRIMES

1 Receiving, laundering or using money, goods or benefits of illicit origin, and self-laundering

Italian Legislative Decree no. 231 of 21 November 2007[11] (the so-called "Anti-Money Laundering Decree") added to the list of offences provided for by Italian Legislative Decree no. 231/2001, under Section 25-*octies* the crimes of receiving (Article 648 of the Criminal Code), laundering (Article 648-*bis* of the Criminal Code) and using of money, goods and benefits of illicit origin (Article 648-*ter* of the Criminal Code), described below.

- **Receipt (Article 648 of the Criminal Code)**

"Apart from cases of complicity in the offence, whoever, in order to procure a profit for themselves or for others, receives or conceals money or goods resulting from any crime, or in any case intervenes in order that such be acquired, received or concealed, shall be punished with imprisonment for a term of between two and eight years, and a fine of between € 516 and € 10,329. The punishment shall be imprisonment for up to six years and a fine of up to € 516, if the offence is of a particularly tenuous nature. The provisions of this article shall also apply when the perpetrator of the offence from which the money or goods derive, is not indictable."

Fines pursuant to Italian Legislative Decree no. 231/01: from 200 to 800 units. If the money, goods or other benefits derive from a criminal offence which is punishable with imprisonment for a maximum term of more than five years, then a fine of between 400 and 1,000 units shall apply. Moreover, the equivalent value of the price, profit or product of the offence shall be confiscated.

[11] Italian Legislative Decree no. 231/2007 was promulgated in implementation of Directive 2005/60/EC and concerns the prevention of the use of the financial system for the purpose of laundering the proceeds of criminal activities and for financing terrorism.

Bans pursuant to Italian Legislative Decree no. 231/01: 1) a ban on the exercise of the profession; 2) the suspension or revocation of any authorizations, licences or concessions favouring commission of the offence; 3) prohibition to enter into contracts with the Public Administration other than in order to obtain provision of a public service; 4) a ban on the receipt of any benefits, loans, grants or subsidies, and the possible revocation of those already granted; 5) prohibition to advertise goods or services. All for a period of up to two years.

- **Money laundering (Article 648-bis of the Criminal Code)**

"Apart from cases of complicity in the offence, whoever replaces or transfers money, goods or other benefits resulting from an intentional crime, or, in relation to them, carries out other transactions, in order to hinder the identification of their unlawful provenance, shall be punished with imprisonment for a term of between four and twelve years, and a fine of between € 5,000 and € 25,000. The punishment shall be increased when the offence is committed during the exercise of a professional activity. The punishment shall be reduced if the money, property or other benefit derived from a crime for which the maximum punishment prescribed is imprisonment for less than five years. The last paragraph of Article 648 shall apply".

Fines pursuant to Italian Legislative Decree no. 231/01: from 200 to 800 units. If the money, goods or other benefits derive from a criminal offence which is punishable with imprisonment for a maximum term of more than five years, then a fine of between 400 and 1,000 units shall apply. Moreover, the equivalent value of the price, profit or product of the offence shall be confiscated.

Bans pursuant to Italian Legislative Decree no. 231/01: 1) a ban on the exercise of the profession; 2) the suspension or revocation of any authorizations, licences or concessions favouring commission of the offence; 3) prohibition to enter into contracts with the Public Administration other than in order to obtain provision of a public service; 4) a ban on the receipt of any benefits, loans, grants or subsidies, and the possible revocation of those already granted; 5) prohibition to advertise goods or services for a period of up to two years.

- **Use of money, goods or other benefits of illicit origin (Article 648-ter of the Criminal Code), and self-laundering (Article 648-ter.1 of the Criminal Code.)**

Art. 648-ter (Use of money, goods or other benefits of illicit origin)

"Whoever, apart from the cases of complicity in an offence and the cases set forth in Articles 648 and 648-*bis*, uses money, goods or other benefits deriving from crime in financial or economic activities, shall be punished by imprisonment for a term of between four and twelve years and by a fine of between € 5,000 and € 25,000. The punishment shall be increased when the offence was committed in the exercise of a professional activity. The punishment shall be reduced in the case set forth in paragraph 2 of Article 648. The last paragraph of Article 648 shall apply".

Art. 648-*ter*.1 (Self-laundering)

Section 3, paragraph 3, of Italian Law no. 186/2014 has introduced into the Italian legal system, as of 1 January 2015, the new criminal offence of self-laundering, including this new offence in the so-called "list" of offences provided for by Italian Legislative Decree no. 231/2001.

Self-laundering consists in the concealment of the proceeds of one's own criminal offences, such as tax evasion, corruption and embezzlement.

Article 648-*ter*.1 establishes the following: "punishment of imprisonment from 2 to 8 years and a fine of € 5,000 to € 25,000 shall be inflicted on anyone who, in committing or being an accessory to, an intentional crime, employs, replaces, transfers, in economic, financial, business or speculative activities, money, goods or other benefits from the crime, in such a way as to concretely hinder the identification of their criminal origin. Punishment of imprisonment for a term of 1 to 4 years and a fine of € 2,500 to € 12,500 shall be inflicted if the money, goods or other benefits derive from an intentional crime which is punishable with imprisonment for a maximum term of less than 5 years.

The penalties provided for by the first paragraph shall be applied, however, if the money, goods or other benefits derive from an offence committed under the conditions or for the purposes referred to in Section 7 of Italian Decree Law no.

152 of 13 May 1991, converted, with amendments, by Italian Law no. 203 of 12 July 1991 and subsequent amendments thereto.

With the exception of the cases referred to in the previous paragraphs, those cases in which the money, goods or other benefits are employed for mere personal use or enjoyment, are not prosecutable.

The penalty shall be increased if the offences are committed in the exercise of banking and financial activities or other professional activity.

Moreover, provision is made for the halving of the penalty for those who effectively cooperate to prevent the conduct from resulting in further consequences, or to guarantee proof of the crime and the identification of goods, money and other benefits deriving from the crime. The final paragraph of Article 648 shall apply".

Fines pursuant to Italian Legislative Decree no. 231/01: from 200 to 800 units. If the money, goods or other benefits derive from a criminal offence which is punishable with imprisonment for a maximum term of more than five years, then a fine of between 400 and 1,000 units shall apply. Moreover, the equivalent value of the price, profit or product of the offence shall be confiscated.

Bans pursuant to Italian Legislative Decree no. 231/01: 1) a ban on the exercise of the profession; 2) the suspension or revocation of any authorizations, licences or concessions favouring commission of the offence; 3) prohibition to enter into contracts with the Public Administration other than in order to obtain provision of a public service; 4) a ban on the receipt of any benefits, loans, grants or subsidies, and the possible revocation of those already granted; 5) prohibition to advertise goods or services for a period of up to two years.

2 Areas at risk from the commission of offences

The potential risk areas that Banca Sistema has identified within the context of the crimes of receiving, laundering and use of money, goods and other benefits of illicit origin, are those pertaining to:

a. the acquisition without recourse of receivables payable by the National Health Service;
b. the opening of current accounts and the formalities established for the due verification of customers;
c. the provision of financial and investment services to the Bank's customers;
d. the negotiation, conclusion and performance of proxy, brokerage, consultancy, agency and financial advisory agreements;
e. the development, promotion and management of humanitarian and solidarity projects;
f. the selection of business/financial partners and the management of the corresponding relations with such;
g. the management of relations with suppliers;
h. the establishment of the means of payment;
i. the management of investments (such as, for example, acquisition of shareholdings or companies, strategic agreements, other extraordinary financial transactions);
j. the undue receipt of public subsidies;
k. pawn credit.

Any amendments or additions to the aforementioned risk areas shall be the responsibility of the Board of Directors, also upon proposal from the SB.

The Bank has also adopted its own specific anti-money laundering policy, approved by the Board of Directors, and has appointed a person in charge of this matter. Moreover, it has made provision, in accordance with the 15th update, dated 3 July 2013, of Bank of Italy Circular no. 263/2006, for the monitoring of the risk of non-compliance with tax regulations by the Compliance/Anti-Money Laundering.

3 Rules of Conduct

In the performance of their duties/functions, as well as being aware of, and complying with, the rules laid out in the Anti-Money Laundering Decree and the Bank's Articles of Association, operating procedures and all other internal rules

pertaining to the Corporate Governance system, the Recipients must also comply with the rules of conduct set out in this Model.

More specifically, this Special Part expressly prohibits:

1. engaging in any form of conduct that may give rise to one of the aforementioned criminal offences (pursuant to Section 25-*octies* of the Decree), or in any form of conduct which although in itself does not constitute an offence, may in theory give rise to the commission of one of the offences in question;
2. business relations with persons (natural or legal persons) who are known to be, or are suspected of being, members of a criminal organization, or who operate outside of the law, such as, for example, persons connected to the worlds of money laundering, terrorism, drug trafficking, usury, etc.;
3. the use of instruments that do not follow a procedure, for transactions involving the transfer of substantial sums;
4. accepting contractual relations with customers or other contractual counterparties with registered offices or place of residence in, or any connection with, countries considered as non-cooperating by the FATF[12];
5. giving money to individuals, companies or organizations that have been found guilty of carrying out illegal activities, in particular terroristic or subversive activity.

Furthermore, the Recipients are bound:

1. in regard to the business/professional reliability of suppliers and partners, to ask for all the information required in order to assess the reliability and financial soundness thereof;
2. to ensure that all payments have been regularly made: in particular, they must check to ensure that the persons to whom the orders are made out to are the same persons who collect the corresponding sums;

[12] Established in 1989 at the time of the Paris G7, the Financial Action Task Force (FATF) is an intergovernmental organization whose aim it is to develop strategies to combat illicit money-laundering, and since 2001 to combat the financing of terrorism.

3. to behave in good faith and in a correct, transparent, cooperative manner, in accordance with the provisions of law and of company procedures, in all activities aimed at the handling of suppliers and customers' details;
4. to take particular care with regard to payments received from foreign banks/customers.

With regard to the identified risk areas, the Bank must comply with the following specific rules of conduct, already governed by Italian Legislative Decree no. 231/2007, in observance of the Decree:

a. the Bank must create specific records of customers and suppliers, containing the most important information regarding them (for example, details of their legal representative, country of residence, type of business, company financial statements for the last two years, etc.) also in order to establish that the Bank's counterparties meet the respectability and professionalism requirements;
b. the Bank must select suppliers and business partners in such a way as to permit an objective, transparent comparison of all offers based on objective, verifiable criteria, by verifying the commercial solidity of such suppliers and partners (for example, through: company searches at the Chamber of Commerce, or equivalent company certificates from foreign jurisdictions; references from other persons who already have a business relationship with the Bank, or public institutions or professional associations or highly-reputed professional firms; anti-mafia certificates, certificates of pending proceedings against directors, or equivalent certificates from foreign jurisdictions);
c. the Bank must not accept or make payments in cash other than those below a certain limit, and in any case always within the limits established by law;
d. the Bank constantly monitors company financial flows, paying specific attention to the origin of any payments; these controls must take account of the registered office of the contractual counterparty (e.g. tax havens, countries at risk from terrorism), of the banks used (the registered offices of the banks involved in the transactions), and of any trust companies utilized for extraordinary transactions or operations;

e. in the event of cash donations to individuals, companies or organizations, the worthiness and professionalism of the individuals in question must be verified. Moreover, an investment plan must be drawn up, justifying the investment, and the state of progress of said plan must be checked regularly;
f. the Bank shall verify, ex ante, that the persons with whom it has contractual relations, including employment relations, are not on the anti-terrorism black list.

Any agreements with contractors who have dealings with the Public Administration must contain a clause governing the consequences of said contractors' failure to fulfil their obligations under the Decree and the ethical principles established by the Model.

4 The Supervisory Body's duties

Without prejudice to the SB's discretionary power to carry out specific controls following reports received (see the provisions of the General Part of this Model), it is the SB's duty to:

a. carry out regular controls regarding compliance with this Special Part, and to evaluate its effectiveness in preventing the commission of the offences set out in Section 25-octies of the Decree;
b. propose and cooperate with the preparation of control procedures pertaining to the conduct to be followed within the risk areas referred to in this Special Part, together with the other control functions;
c. check that personnel are given due training in the field of anti-money laundering.

To this end, the SB shall be guaranteed free access to all relevant company documents.

Depending on the violation discovered, Section 52 of Italian Legislative Decree no. 231/2007 establishes that the SB must send an internal communication to the Entity, addressed to the legal representative or to his/her proxy (letter b), or a communication addressed to bodies outside of the Entity, and specifically to

the Supervisory Authority for the sector in question (the Bank of Italy) and to the Ministry of Economy and Finance (letters a), c) and d)). The aforesaid reports may be made jointly with other company bodies or functions.

E) COMPUTER CRIMES AND UNLAWFUL PROCESSING OF DATA

1 Computer crimes and unlawful processing of data

The Council of Europe's Convention on Cybercrime, signed in Budapest on 23 November 2001, constitutes the first international agreement on crimes committed through the Internet or other computer networks. Said Convention aims to establish a common policy on the issue among member states, through the adoption of appropriate legislation enabling computer crime to be combated in a coordinated manner.

The Italian legislator ratified the aforesaid Convention with Law no. 48 of 18 March 2008, which introduced a series of significant changes to Italy's body of law from both the substantive and the procedural point of view.

Knowledge of the nature of the crimes and of the way in which they are committed by those persons identified by Section 5 of Italian Legislative Decree no. 231/2001, which is related to the entity's system of liability, is of fundamental importance for the prevention of such crimes, and thus for the entire system of controls provided for by the Decree.

The breadth of the changes introduced also affected Italian Legislative Decree no. 231/01, which on the basis of the provision laid down in the new Section 24-*bis*, endorses the prosecutable nature, pursuant to the aforementioned Decree, of those criminal offences identified by the amended Articles of the Criminal Code, if the offences in question are committed by the entity's employees, by persons equivalent to such, or by senior figures within the entity, also in the interest and/or for the benefit of the entity itself.

Computer crimes include a variety of criminal offences where a computer system in certain cases represents the direct subject-matter of the offence, and in other cases where it represents the means by which the perpetrator aims to commit another criminal offence.

The development of computer technology has produced, over the course of the years, a number of substantial changes to the ways that companies' business is organized, and has significantly affected the opportunities available to each representative of a company to carry out, or to conceal, not only existing forms of criminal activity, but also new types of criminal offences characteristic of the so-called "virtual world".

It should be pointed out that the Bank utilizes a computer and telecommunications system designed to handle the complex operating and regulatory environment in which it does business, as expressly required by, among others, the specific regulations governing this sector. Within this context, the management of the Bank's computer system (Application Management and Facility Management) is entirely outsourced to an external supplier (Consorzio Servizi Bancari).

The following is a brief description of the offences referred to in Section 24-bis of Italian Legislative Decree no. 231/2001, the control protocols pursuant to which were established during the updating of this Organizational Model.

- **Forgery of an official electronic document or a private electronic document of evidential value (Article 491-bis of the Criminal Code)**

The provisions of the Criminal Code regarding the forgery of hard-copy documents have been extended to cover electronic documents: the latter term means any electronic document containing data or information of evidential value, or the programmes specifically designed to process such data or information.

Article 491-*bis* of the Italian Criminal Code provides a definition of electronic document based on the material element of digital memory media, and not on the data contained therein; electronic storage media may be any memory media – located either inside or outside a computer – on which data to be read and, if necessary, processed by a computer system may be recorded and stored for a certain period of time.

Pursuant to Article 491-bis of the Italian Criminal Code, electronic storage media do not include the printout produced by a computer at the end of a data

processing procedure: the printout – as is the case with all printed material – is in fact normally constituted by a sheet of paper on which the data are reproduced in letter and numerical form so that people can read them; on the other hand, the concept of electronic document includes payment cards with a magnetic strip, and microprocessor cards (e.g. prepaid cards, top-up cards and telephone cards).

Electronic documents also include the electronic storage media containing the programme specifically designed to process the data, that is, the programme memorized inside a computer system or on an external medium that processes the data.

- **Unauthorised access to a computer or telecommunication system (Article 615-ter of the Italian Criminal Code)**

"Whoever unlawfully accesses a computer or telecommunication system protected by security measures, or maintains access to such against the express or tacit will of those who have the right to exclude them from such access, is punished with imprisonment for up to three years.

Imprisonment shall be for a term of from one to five years:

1) *if the offence is committed by a public service official or a person in charge of a public service, by abusing their powers or breaching their obligations regarding the function or the service, or by anyone who unlawfully exercises the profession of private investigator, or by anyone abusing their powers as system operator;*
2) *if the offender uses violence against property or persons in committing the offence, or if such person is patently armed;*
3) *if the offence results in the destruction or the damaging of the system, or the total or partial interruption of its operation or the destruction or damage of the data, information or programmes contained therein.*

Should the offences referred to in points 1) and 2) above concern computer or telecommunication systems of military interest, or related to public order, public security, the health service or civil defence, or in any case of public interest, the

penalty shall be imprisonment for a term of between one and five years, and for a term of between three and eight years, respectively.

In the case referred to in point 1), the crime may be punished subject to the offended person taking legal action; in the other cases, legal action is taken automatically".

This provision is designed to safeguard the confidentiality of the data and the programmes contained in a computer system.

The term "computer system", for the purposes of the offence referred to in Article 615-*ter* of the Criminal Code, means several devices designed to perform a function of use to people, through the utilization, even only partial, of information technologies. The system is thus described as such if it can handle and process data, whereas everything that is contained in a website or in the IT world, that is not capable of managing or processing data in order to perform a function, cannot be considered a computer system.

Unauthorized access occurs as soon as the system's security safeguards are got around, that is, all of those protective measures which, when got around, provide access to the data and programmes contained in the system, such as alphabetical or numerical access codes to be entered using a keyboard, or stored on the magnetic strip of a card to be inserted into a card reader. In addition to these logical measures of protection, there are also physical means such as the use of metal keys to switch on the computer.

The offence in question consists in unlawfully accessing a computer or telecommunication system protected by security measures, or in maintaining access to such against the express or tacit will of those who have the right to exclude others from such access. Such access occurs when a person goes beyond the logical and/or physical barriers safeguarding access to the system's internal memory, and thus has the opportunity to recall the data and programmes contained therein. Unauthorized access may be gained both remotely, that is, by electronic means, or from close proximity by the person in direct contact with the computer.

In addition to unauthorized access, there is also the offence of maintaining a presence in a protected system against the express or tacit will of those who have the right to exclude others from such access: this offence occurs when following unintentional, casual or only initially authorized access, the person in question remains in the computer system of another notwithstanding the objections of the person who has an interest in the confidentiality of the data and programmes contained therein.

It should be pointed out that the term "system operator" refers exclusively to the IT technical expert (system administrator) who has control, within a company, over the various phases of date processing operations, and the opportunity to access all sectors of the memory of the computer system he/she works with, or that of other systems if there is a network connection.

- **Unauthorised possession or disclosure of access codes for IT or telecommunications systems (Article 615-quater of the Criminal Code)**

"Whoever, in order to obtain a profit for themselves or cause damage to others, unlawfully obtains, reproduces, circulates, communicates or delivers codes, key words or other means for accessing an IT or telecommunications system protected by security measures, or in any case gives indications or instructions for such purpose, shall be punished with imprisonment for a term of up to one year and a fine of up to € 5,164".

The penalty shall be imprisonment for a term of one to two years and a fine of between € 5,164 and € 10,329 if one of the circumstances provided for at points 1) and 2) of the fourth paragraph of Article 617-quarter arises.

Article 615-*quater* aims to punish the unlawful detention and disclosure of access codes that may lead to the commission of other computer crimes: in fact, whoever unlawfully obtains access codes may commit the offence of unlawful access to a system, or may disclose said codes to other persons who in turn could gain unlawful access to the system.

The object of the offence is any means enabling the perpetrator to get around the IT system's protection, regardless of the nature of such means: it may

consist in a password, an access code or simply information enabling the protective measures to be got around.

The provision in question punishes two forms of conduct: the first, aimed at the acquisition of the means required to gain access to the IT system, while the second is aimed at procuring such means for others, or at obtaining for others the information required to get round the protective barriers; the mere unauthorized detention of access codes or similar instruments, on the other hand, is not prosecutable.

- **Distribution of equipment, devices or computer programmes aimed at damaging or interrupting a computer or telecommunications system (Article 615-quinquies of the Criminal Code)**

"Whoever, in order to damage a computer or telecommunications system, the information, data or programmes contained therein or pertaining thereto, or to facilitate the total or partial interruption or alteration of its functioning, manages to communicate, deliver or make available to others in any other way any computer programmes that he/she has created, or that have been created by others, shall be punished with imprisonment for a term of up to two years and a fine of up to € 10,329".

Article 615-*quinquies* of the Criminal Code is designed to protect electronic assets - meaning hardware, software and data – against attack from computer viruses.

The prosecutable conduct is the diffusion (disclosure), the communication (informing people) or the delivery (material provision) of a computer programme that is designed to damage, or results in damaging, another's computer or telecommunications system, or the data or information contained therein or pertaining to such, or to partly or totally hinder, or alter, the functioning of such system.

The law makes no distinction between viruses created by the perpetrator of the offence and those created by others, nor indeed between a computer programme that actually causes damage to a computer system, and one that does not cause such damage.

A programme may be defined as infected for the purposes of the provision in question, if it is capable not only of damaging the logical components of a computer system, but also of interrupting or altering its functioning.

- **Illegal interception, prevention or interruption of communications on a computer or telecommunication system (Article 617-quater of the Criminal Code)**

"Whoever fraudulently intercepts communications on a computer or telecommunication system, or between several interconnected systems, or prevents or interrupts such communications, shall be punished with imprisonment for a term of between six months and four years.

Unless the act constitutes a more serious offence, the same punishment shall be inflicted on anyone who publicly discloses, by any means of communication, wholly or in part, the contents of the communications referred to in the first paragraph.

The offences referred to in paragraphs one and two are prosecutable upon the filing of a complaint by the injured party.

Nevertheless, the offence shall be prosecuted automatically, and shall be punished with imprisonment for a term of between one and five years, if it has been committed:

1) *to the detriment of the computer or telecommunication system used by the State or by another Public Entity, or by an undertaking providing essential or other public services;*
2) *by a public official or a public service agent, through the abuse of such person's powers or in breach of his/her duties pertaining to the function or service in question, or through the abuse of his/her capacity as system operator;*
3) *by whoever exercises, legally or otherwise, the profession of private investigator".*

For the purposes of the provision in question, the offence may consist, alternatively, in fraudulently intercepting a computer or IT communication, or in preventing or interrupting such communication; the second paragraph then deals

with the public disclosure, by any means of communication, wholly or in part, of the contents of an intercepted conversation.

Intercepting a computer or IT communication means discovering its contents by intervening during its transmission; said interception must be carried out fraudulently, that is, by getting round any systems protecting the ongoing transmission (e.g. by decoding data transmitted in a coded form, or overcoming any logical barriers created to protect the system that sends or receives the communication), or in such a way that the unauthorized intervention is imperceptible or unrecognizable to others.

The communication is prevented, on the other hand, when transmission is rendered impossible through interference in the computer system that is to send or receive the data; finally, a communication may be interrupted both by operating on the system that sends or receives the communication, and by deviating the flow of data being transmitted, from one computer to another.

- **Installation of equipment designed to intercept, prevent or disrupt computer or electronic communications (Article 617-*quinques* of the Criminal Code)**

"Whoever, except in cases permitted by law, installs equipment designed to intercept, prevent or disrupt communications on a computer or electronic system, or between several interconnected systems, shall be punished with imprisonment for a term of between one and four years.

The punishment shall be imprisonment for a term of between one and five years in those cases provided for under the fourth paragraph of Article 617-quarter".

This provision aims to contain an offence committed prior to, and in preparation for, the offence provided for under Article 617-*quater* of the Criminal Code, by forbidding the unlawful installation of devices designed to intercept, prevent or interrupt computer communications.

The offence provided for by Article 617-*quinquies* of the Italian Criminal Code has been identified in the case of the utilization of devices capable of copying the access codes of users of a computer system, given that the unlawful copying of access codes for the initial communication with the system falls within the notion of "interception" referred to in the incriminatory provision.

- **Damaging computer information, data and programmes (Article 635-bis of the Criminal Code)**

"Unless the fact constitutes a more serious offence, whoever destroys, deteriorates, deletes, alters or suppresses computer information, data or programmes belonging to others shall be liable, upon complaint by the injured party, to a term of imprisonment of from six months to three years.

If one or more circumstances referred to in the second paragraph of Article 635 apply, or if the fact is committed by abusing the status of system operator, the penalty shall be imprisonment for a term of from one to four years".

The object of the damage may be, firstly, a computer system of any type and size, which may be remotely connected to other computers as in the case of telecommunication systems. The attack may be against the entire system, or against one or more of its physical components, such as its peripheral devices. However, magnetic or optical media on which data or programmes are stored cannot be considered components of a computer system since, should they be damaged, this would not impede in any way the functioning of the computer system in which they are to be utilized.

As well as to the computer system as such, damage may also be caused to computer data and programmes: data means those representations of information or concepts that, being due for processing by the computer, are codified in a form (electronic, magnetic, optical or similar) that is not visibly perceptible. Data or programmes stored in the computer's internal memory, or on an external device such as a magnetic or optical disk, may also be susceptible to damage.

The assets susceptible to damage pursuant to Article 635-*bis* of the Criminal Code also include information: since information is in itself an abstract entity, this expression only has any meaning insofar as it refers to the information incorporated onto a physical medium, hard-copy or another medium.

The forms of conduct that may constitute the offence in question are the partial or complete destruction, deterioration or unserviceability of such information, data or programmes. The commonest, most important case of the destruction of

data and programmes is that of their deletion, whether this be the result of the demagnetizing of the medium, or of the replacement of the original data with different new data, or of the computer containing the data or programmes being given a command capable of causing the data or programmes to disappear. Given that destruction must be total, this offence is not committed if the cancelled data or programmes are still recoverable in a remote area of the computer, by using a certain type of programme, or if such simply cannot be seen on the computer's screen.

- **Damaging computer information, data or programmes used by the State or by another public authority, or in any case useful to the public (Article 635-ter of the Criminal Code)**

"Unless the offence in question constitutes a more serious offence, whoever commits an offence designed to destroy, deteriorate, delete, alter or suppress computer information, data or programmes used by the State or by another public authority or pertinent to them, or in any case useful to the public, shall be liable to a term of imprisonment from one to four years.

If the offence results in the destruction, deterioration, deletion, alteration or suppression of computer information, data or programmes, the penalty shall be imprisonment for a term of from three to eight years.

If the circumstance referred to in number 1) of the second paragraph of Article 635 arises, or if the fact is committed by abusing the status of system operator, the penalty shall be increased".

For a description of the elements constituting the offence in question, see the preceding offences.

- **Damaging computer or telecommunications systems (Article 635-quater of the Criminal Code)**

"Unless the offence in question constitutes a more serious offence, whoever, through the forms of conduct referred to in Article 635-bis, or by introducing or transmitting data, information or programmes, destroys, damages or renders unserviceable, either completely or partially, computer systems belonging to

others or seriously obstructs their functioning, shall be liable to imprisonment for a term of from one to five years.

If the circumstance referred to in number 1) of the second paragraph of Article 635 arises, or if the fact is committed by abusing the status of system operator, the penalty shall be increased".

For a description of the elements constituting the offence in question, see the preceding offences.

- **Damaging computer or telecommunications systems of public interest (Article 635-quinquiesof the Criminal Code)**

"If the offence referred to in Article 635-quater of the Criminal Code is aimed at destroying, damaging or making computer or telecommunications systems of public interest unserviceable, or at obstructing their functioning, the penalty shall be a term of imprisonment from one to four years.

If the offence results in the destruction of, or damage to, computer or telecommunications system of public interest, or if this is rendered, in whole or in part, unserviceable, the penalty shall be imprisonment for a term of from three to eight years.

If the circumstance referred to in number 1) of the second paragraph of article 635 arises, or if the offence is committed by abusing the status of system operator, the penalty shall be increased".

For a description of the elements constituting the offence in question, see the preceding offences.

- **Computer fraud by individuals providing electronic signature certification services (Article 640-quinquies of the Criminal Code)**

"Individuals providing electronic signature certification services who, in order to gain an unjust profit either for themselves or for others, or to cause damage to others, violate the obligations provided for by the law concerning the issuing of authorized certificates, shall be liable to imprisonment for a term of up to three years and a fine ranging from € 51.00 to € 1,032.00".

European Directive 1999/93/EC, transposed by Italian Legislative Decree no. 10 of 23 January 2002, governs the use of electronic signatures within the EU, with the aim of promoting their use and legal recognition, through the introduction of systematic rules regarding the subject, and of certain certifying services that guarantee the correct operation of said electronic signatures. Several national regulatory measures have been adopted to promote the effective adjustment of national provisions to bring them into line with EU regulations, and these have led to the promulgation of the Digital Administration Code (Italian Legislative Decree no. 82/2005, partially amended by Italian Legislative Decrees nos. 159/2006 and 235/2010) which currently constitutes the primary source of legislation in this field.

2 Areas at risk of crime

An analysis of Banca Sistema's corporate processes has made it possible to identify those activities within the context of which the offences referred to in Section 24-bis of Italian Legislative Decree no. 231/2001 could in theory be committed. Hence, the following is a list of the so-called "sensitive activities" or "risky activities" identified by said analysis with regard to computer crimes.

1) management of user profiles and of the authentication process;
2) management of the creation, processing and storage of electronic documents of evidential value;
3) management and protection of work stations;
4) management of accesses to and from the outside;
5) management and protection of networks;
6) physical safety (including the safety of cabling, network devices, etc.).

3 Rules of Conduct

The system of controls created by Banca Sistema establishes, with regard to the aforesaid sensitive activities:

- the General principles of control regarding sensitive activities;

- specific protocols to be applied to individual sensitive activities.

General principles of control

The general principles of control underlying the instruments and methods used to realise the specific control procedures may be summarized as follows:

- Formalised procedures/guidelines. Provision is made for internal regulations (company policies, procedures, etc.) and for external regulations (laws, regulations, supervisory provisions, etc.) capable of providing principles of conduct and operating methods for the carrying out of sensitive activities, together with methods of storing relevant documents.
- Segregation of duties: the principle of separation of activities between those who authorize, those who perform, those who record and those who control transactions, so as to guarantee the independence and objectivity of the processes in question;
- The existence of a system of proxies and powers of attorney consistent with the assigned organisational responsibilities. Authorising and signatory powers must: a) be consistent with the assigned organisational and management responsibilities and, if required, provide for the specification of limits of expenditure approval; b) be clearly defined and known within the Bank;
- Traceability and ex-post accountability of transactions through adequate documents/IT means. Each transaction carried out within the context of a sensitive activity must be adequately documented and registered. The process of decision-making, authorization, performance and control with regard to the sensitive activity must be verifiable ex-post, also with the aid of specific documents, and in any event, the cases of, and the procedures for, a possible cancellation or elimination of the registration made must be regulated in detail.
- Monitoring activities designed to permit the regular/prompt updating of delegated powers and of the control system. The appointed departments,

supported by other departments, shall regularly monitor the system of delegated powers and proxies in force, verifying their consistency with the decision-making system, as well as the entire organizational structure, recommending any modifications required, such as, for example, when the managerial power and/or the qualification fail to correspond to the representative powers assigned to the delegate, or when other anomalies have been identified.

Specific principles of control

The main methods of carrying out controls regarding the previously-mentioned sensitive activities, may be summarized as follows:

- Security policy. The security provisions addressed to the Banks' personnel and to external personnel (suppliers and third parties) who access company information, are laid out in the Security Policy Document.
- Organization of security for users. The Bank has laid down specific internal instructions governing the conduct of employees when using IT instruments, and has adopted security rules designed to guarantee the confidentiality, integrity and availability of processed information. With regard to the processing of personal data protected by privacy regulations, data processors have been appointed for the various company functions, together with persons in charge of processing, who have been given the necessary instructions.
- Physical and environmental security. Access to premises is monitored by physical security devices, with entry controlled by means of badges, and by alarm systems. The Bank's server rooms, located in the supplier's premises, are subject to the physical safety measures, procedures and operating instructions set out in the corresponding contract: in particular, physical segregation devices are adopted, with controlled access and authentication mechanisms that permit only authorized personnel to operate. Furthermore, the server room is also fitted with the main

environmental safety devices for fire prevention and dealing with power outages.

- Management of communications and operability. The Bank's computer system is protected against unauthorized external access, by means of firewall systems and perimeter security devices that separate the company environment from the outside. Numerous measures are in place that limit Internet access, block off spam, and protect the system from dangerous software, through the installation of antivirus programmes that are automatically updated by a central server that distributes virus signatures both to the servers and to individual computers. A record is kept of access to data, and of operations performed, by both application users and by system administrators, and any attempts to modify systems and applications, even in emergencies, are traceable.
- Access control. User enablement/modification/disablement is performed by the Bank's IT structure upon request from the Personnel Office, on the basis of proven procedures. Access to the corporate network and to the computer systems is provided by means of individual ID codes assigned to each individual user, and managed in such a way that they are disabled should the user lose entitlement to access data (e.g. following dismissal or job rotation), or in the event of non-use of such codes.

  Control of access to the Bank's application services is governed by a contract with the appointed supplier (CSE); access to such services is by user IDs and passwords permitting authentication exclusively to those persons with the necessary authorization.
- Management of IT security incidents and issues. The analysis of security incidents and problems regarding application services, is carried out by the Bank with the support of the outsourcer (CSE) which uses an incident management system. The adopted internal rules establish that the supplier shall report the incident to the Bank in order that the problem be resolved, in accordance with proven procedures. In the event of

malfunctions, an incident report is generated that describes the identified anomaly and the solutions adopted.

- Security in the acquisition, development and maintenance of information systems. The development and maintenance of the Bank's central computer systems are governed by the contract stipulated with the appointed supplier (CSE).

  The release of software updates follows a standard operating procedure establishing clearly defined activities and responsibilities. The updating of basic software and of management and control software is carried out by the outsourcer.

  The development of Banca Sistema's computer systems, on the other hand, is handled by the IT Office, on the basis of specific procedures, authorizing workflows and standard instruments for all applications handled.
- Audit. The Annual Internal Audit Plan provides for regular technical and organizational audits of security policy, and of the methods of assignment and amendment of the accounts. Furthermore, each year an IT audit of the computer systems used is conducted at the outsourcer (CSE), by an independent firm appointed by the "associated" banks. The results of said audits are regularly and promptly shared with the Supervisory Body.

In addition to the aforementioned principles, the Bank has also adopted other governance instruments, described in the Model (General Part), such as the system of delegated powers, documents regarding the organisational structure, Policies, Internal Regulations, and the Security Planning Document.

4 The Supervisory Body's duties

The offences provided for in this Special Part are monitored by means of specific IT audits conducted regularly by the Bank's Internal Audit function, on its internal IT systems. The audits of IT processes provided by the outsourcer (CSE) of the Bank's management systems shall be conducted annually by an

independent consultancy firm appointed by the banks that use the provider. The results shall be shared among said banks.

F) OCCUPATIONAL HEALTH AND SAFETY OFFENCES

1 Occupational health and safety offences

The following occupational health and safety offences may result in the administrative liability of the Entity pursuant to Section 25-*septies*[13] of Italian Legislative Decree no. 231/2001:

- **Manslaughter (Article 589 of the Criminal Code)**

"Whoever negligently causes the death of an individual is liable to imprisonment for a term of from six months to five years. If the fact is committed in violation of road safety regulations or occupational health and safety rules, the penalty shall be imprisonment for a term of from one to five years. In case of death of more than one person, or death of one or more persons and injury to one or more persons, the applicable penalty shall be the one applied to the most serious offence committed increased by up to three times. However, the penalty shall not exceed twelve years."

Fines pursuant to Italian Legislative Decree no. 231/01: with regard to the offence governed by paragraph one of Section 25-septies of the Decree, the fine shall be up to 1,000 units; in the case of the offence referred to in paragraph two of Section 25-septies of the Decree, the fine shall be between 250 and 500 units.

Bans pursuant to Italian Legislative Decree no. 231/01: 1) a ban on the exercise of the profession; 2) the suspension or revocation of any authorizations, licences or concessions favouring commission of the offence; 3) prohibition to enter into contracts with the Public Administration other than in order to obtain provision of a public service; 4) a ban on the receipt of any benefits, loans, grants or subsidies, and the possible revocation of those already granted; 5) prohibition to advertise goods or services. In the case of the offence referred to in paragraph one, for a period of up to one year. In the case of the offence referred to in paragraph two, for a period of between three months and one year.

- **Unintentional personal injury (Article 590, paragraph 3, of the Criminal Code)**

"[…] If the offences referred to in the second paragraph are committed in violation of road safety regulations or occupational health and safety rules, the penalty for serious injuries shall be imprisonment for a term of from three months to one year or a fine of from € 500.00 to € 2,000.00, and the penalty for very serious injuries shall be imprisonment for a term of from one to three years. In the case of violation of road safety regulations, if the offence is committed by an individual driving under the influence of alcohol pursuant to Section 186, paragraph 2, letter c), of Italian Legislative Decree no. 285 of 30 April 1992 and subsequent amendments, or by an individual driving under the influence of narcotic drugs or psychotropic substances, the penalty for serious injuries shall be imprisonment for a term of from six months to two years, while the penalty for very serious injuries shall be imprisonment for a term of from one year and six months to four years.

Fines pursuant to Italian Legislative Decree no. 231/01: up to 250 units.

Bans pursuant to Italian Legislative Decree no. 231/01: 1) a ban on the exercise of the profession; 2) the suspension or revocation of any authorizations, licences or concessions favouring commission of the offence; 3) prohibition to enter into contracts with the Public Administration other than in order to obtain provision of a public service; 4) a ban on the receipt of any benefits, loans, grants or subsidies, and the possible revocation of those already granted; 5) prohibition to advertise goods or services for a period of up to six months.

2 Areas at risk of crime

The Guidelines set out by Confindustria (the Federation of Italian industrialists and entrepreneurs) concerning the offences dealt with in this Special Part, reveal the impossibility of excluding, *a priori*, any of the company's areas of activity,

[13] Article added by paragraph 9 of Italian Law no. 123 of 3 August 2007, and amended by Italian Legislative Decree no. 81/08.

since the offences in question could regard all cases in which there is a breach, within the company, of its occupational health and safety obligations.

Consequently, the potential risk areas identified by the Bank in relation to said offences concern all of the operations conducted by Banca Sistema, as well as those carried out by external personnel (e.g. service providers on the basis of tender contracts, work contracts or supply contracts). Special attention must be paid to those operations carried out in conjunction with partners, or through the conclusion of supply contracts, tender contracts, or contracts with consultancy firms or freelancers.

The risk factors reported in the "Risk Assessment Document" (hereinafter "RAD") thus need to be taken into consideration also for the purpose of drafting this Special Part, bearing in mind that said risk factors do not exhaust the procedures provided for below, designed to constitute the complete occupational safety management system and to implement Section 30 of Italian Legislative Decree no. 81/2008 in accordance with the principles set forth in the UNI – INAIL Guidelines and in the British Standard OHSAS 18001.

3 Rules of Conduct

With regard to the failure to observe occupational health and safety regulations, which may lead to a damaging event occurring in one of the aforementioned sensitive areas, it is particularly important:

a) that the Board of Directors, upon the recommendation of the Health and Safety Officer, and jointly with the Supervisory Body, establishes the occupational health and safety policies designed to determine the Bank's general undertakings for the prevention of risks and for the gradual improvement of health and safety;

b) that the Board of Directors, upon the recommendation of the Health and Safety Officer, and jointly with the SB, identifies and complies with the technical-structural legal standards governing equipment, systems,

workplaces, chemical/physical/biological agents, and with all provisions of occupational health and safety laws and regulations;

c) that the Board of Directors, upon the recommendation of the Health and Safety Officer, and jointly with the SB, identifies and assesses the risks for all categories of workers, paying specific attention to the drafting of:
   - the RAD;
   - tender contracts;
   - the assessment of risks deriving from interference (Single Document on the Assessment of Interference Risk);
   - Safety and Coordination Plans, Works Dossier and Safety Operating Plans, in those cases where the Bank also takes part in construction activities;

d) that all occupational health and safety measures, provided for in the case of the construction of temporary or mobile building sites, or in any place where building of civil engineering works are being carried out, are duly complied with;

e) that the Board of Directors, upon the recommendation of the Health and Safety Officer, and jointly with the SB, establishes targets in keeping with the general undertakings set out in the policies as per point a), and prepares programmes for achieving such targets, with priorities clearly indicated together with deadlines and the assignment of the corresponding responsibilities – and the assignment of the necessary resources – regarding occupational health and safety, with specific reference to:
   - the assignment of tasks and duties;
   - the activities of the Health and Safety Service and of the Appointed Doctor;
   - the activities of all others responsible for implementation of occupational health and safety measures;

f) that the SB makes all levels of the company's organization aware of the importance of the set targets, in order that such may be reached, also through the preparation of training programmes concerning, in particular:
   - monitoring, periodicity, utilization and learning;

- specific training for the persons exposed to specific risks;

g) that the SB implements suitable monitoring, verification and inspection measures in order to guarantee the effectiveness of the aforementioned occupational health and safety management system, in particular with regard to:

- support and improvement measures;
- the management, adjustment and prevention of conduct engaged in, in breach of regulations, entailing disciplinary provisions;
- the carrying out of activities in keeping with the powers held;

h) that the Board of Directors, upon the recommendation of the Health and Safety Officer, and jointly with the SB, takes the necessary corrective and preventive measures based on the monitoring results.

In order to permit the implementation of the principles designed to protect workers' health and safety referred to in Section 15 of the Health and Safety Decree, and in compliance with the provisions of Sections 18, 19 and 20 of the aforesaid Decree, the following has been provided for.

- **Company occupational health and safety policies**

The occupational health and safety policy adopted by the Bank must constitute a benchmark for Recipients and for all those outside of the Bank who have relations with it.

Said policy applies to all Banca Sistema's activities, and it must aim to express the principles underlying each of the company's actions, which everyone must comply with in relation to their respective roles and responsibilities within the Bank, in view of the health and safety of all employees.

Said policy, established in accordance with UNI-INAIL standards, contains:

- a clear statement of the responsibility of the entire corporate organization, from the employer to each individual employee, for the management of the occupational health and safety system, each according to their own powers and duties;

- an undertaking to consider the occupational health and safety system as an integral part of company management which Recipients are to be guaranteed full knowledge of;
- an undertaking to constantly improve health and safety;
- an undertaking to provide the necessary human resources and instruments;
- an undertaking to guarantee that Recipients, insofar as they are concerned, are made aware of their own duties, and duly instructed in the performance thereof, in accordance with occupational health and safety regulations, and assume their own responsibilities in terms of occupational health and safety;
- an undertaking to involve and consult employees, also through the Health and Safety Officer; more specifically, Banca Sistema shall establish adequate ways of guaranteeing the involvement of its employees, also through the Health and Safety Officer, in order to engage in prior consultation with them aimed at identifying and assessing risks, and establishing risk prevention measures, and shall organize regular meetings with employees for such purpose;
- an undertaking to regularly review the occupational health and safety policy adopted, together with the corresponding management system, in order to guarantee their constant appropriateness for Banca Sistema's organisational structure, and their compliance with the corresponding provisions of law and regulations in force;
- an undertaking to establish and circulate within the Bank the Occupational Health and Safety targets and the corresponding plans for their implementation.

This policy is reviewed annually based on system monitoring results.

Such reviews, the results of which shall not necessarily entail any amendments to the aforesaid policy, may also be conducted following specific events or situations that render them necessary.

- **The planning process**

When planning health and safety targets, the Bank:

- establishes targets for the maintenance and/or improvement of the system;
- formulates assessment criteria capable of showing whether targets have been achieved or not;
- prepares a plan for the achievement of each target, identifies those figures/persons involved in the implementation of said plan, and establishes the corresponding duties and responsibilities;
- establishes the necessary resources, including financial resources, and verifies their adequacy in relation to their employment and to the achievement of targets, through the previous year's allocations, and sees to any adjustments to, or deployment of, the resources in question;
- establishes the nature of the regular and final controls of the actual, effective achievement of targets, through verification of completion of the deployment of those resources allocated to the appointed functions.

- **Information, training and documentation**

Information

The information that the Bank reserves for the Recipients, must be easy to understand and must make them duly aware of:

a. the consequences of their own actions that fail to comply with the Bank's Health and Safety system;
b. their respective roles and responsibilities, and of the importance of acting in accordance with the company's health and safety policy and procedures, with any other provisions regarding the Bank's health and safety system, and with the principles set out in this Special Part.

Given the above, and in view of the different roles, responsibilities and skills of Personnel, and the various risks they are exposed to, the Bank has the following information obligations:

- the Bank must provide due information to its Employees and newly hired staff (including agency staff, trainees, and temporary staff) regarding the specific

risks within the company, the consequences of such risks, and the health and safety measures adopted;

- the information provided regarding the handling of first aid, emergencies, the evacuation of personnel and fire prevention must be duly displayed, and minutes must be kept of any meetings held;
- Employees and newly hired staff (including agency staff, trainees, and temporary staff) must be provided with information about the appointment of the Health and Safety Officer, about the Appointed Doctor, and about those members of personnel with specific duties concerning first aid operations, rescue operations, the evacuation of personnel and fire prevention;
- the information and instructions for use relating to the working equipment made available to Employees must be officially documented;
- the Health and Safety Officer and/or the Appointed Doctor must be involved in formulating the information;
- the Bank must organise regular meetings of the functions responsible for occupational health and safety;
- the Bank must involve the Health and Safety Representative in the organization of risk identification and assessment operations, in the appointment of the members of staff in charge of fire prevention, first aid and premise evacuation operations.

All of the aforementioned information activities must be documented, also in the form of specific minutes.

Training

- The Bank must provide suitable health and safety training to all its employees;
- the Health and Safety Officer and/or the Appointed Doctor must be involved in the drawing up of the training programme;
- any training provided must include the distribution of assessment questionnaires;

- training must be in keeping with the risks of the duties that the employee is actually assigned;
- a specific training programme must be drawn up for the employees exposed to serious, immediate risks;
- the employees who change duties, together with transferred employees, must be provided with preventive, additional, specific training, and must be deemed fit for duty by the Appointed Doctor in the event of work or operations characterized by specific risks;
- those appointed to perform specific duties in the health and safety field (employees in charge of fire prevention, evacuation and first aid duties) must receive specific training in such matters;
- the Bank must carry out regular evacuation drills, details of which must be drawn up (minutes of the drill with details of those involved, and of the performance and results of the drill).

All of the abovementioned training activities must be recorded, including in the form of specific minutes, and must be repeated at regular intervals.

In order to render the organizational system adopted for the management of occupational health and safety more effective, the Bank must ensure that the corresponding information is adequately circulated among, and shared with, all Employees.

Therefore, the Bank shall adopt an internal communications system that provides for two different types of information flows:

- bottom-up: this type of information is guaranteed by the Bank through the provision of special report forms to be filled in by Employees, whereby they can submit observations and proposals to their immediate managers regarding possible improvements that could or need to be made to Occupational Health and Safety management;
- top-down: this type of information is designed to inform all Employees of the Occupational Health and Safety management system adopted by the Bank.

To this end, the Bank undertakes to keep all company representatives constantly and fully informed of developments, through regular company statements and the organization of regular meetings.

Documentation

The Bank shall see to storing the following hard-copy or electronic documents:

- employees' medical records, which must be drawn up and updated by the Appointed Doctor, and kept by the employer;
- an accident register;
- the Risk Assessment Document indicating the methods by which risks have been assessed, and containing a programme of maintenance and improvement measures.

The Bank is also called upon to ensure that:

- the Health and Safety Officer, the Appointed Doctor, and those in charge of implementing emergency and first aid measures are officially appointed;
- documentary evidence is provided of workplace inspections carried out jointly by the Health and Safety Officer and the Appointed Doctor;
- a register of occupational illness files is created and regularly updated, providing details of the date and type of illness, the date of issue of any medical certificates, and the date of transmission of the file;
- documents are kept regarding any accident prevention laws, regulations or provisions pertaining to the company's activities;
- documents pertaining to company regulations and agreements are kept;
- the manuals and instructions for the use of machinery, equipment and individual protective devices, supplied by manufacturers, are duly kept;
- should any occupational health and safety management procedures be implemented, hard-copies or electronic copies of such are kept;
- all documents pertaining to Information and Training are kept by the Health and Safety Officer and made available to the SB.

- **Monitoring operations**

The Bank must guarantee the constant, effective monitoring of the occupational health and safety system.

To this end, it must:

- guarantee the constant monitoring of preventive and protective measures prepared for the management of occupational health and safety;
- guarantee the constant monitoring of the adequacy and workings of the occupational health and safety management system, for the purposes of achieving set targets and of ensuring the correct implementation of said system;
- carry out detailed analyses of each workplace accident, in order to ascertain whether there are any gaps in the occupational health and safety management system, and to identify any corrective measures to be taken.

In order to duly perform the aforesaid monitoring operations, the Bank shall avail itself of the services of specialized external resources if the specificity of the field of action calls for such.

4 The Supervisory Body's Duties

Without prejudice to the SB's discretionary power to carry out specific controls following reports received (see the provisions of the General Part of this Model), it is the SB's duty to:

a. carry out regular controls regarding compliance with this Special Part, and to evaluate its effectiveness in preventing the commission of those offences set out in Section 25-septies of the Decree, In this regard, the Supervisory Body – if necessary availing itself of the services of technical consultants with expertise in the field in question - shall regularly analyse the operation of the preventive system adopted with this Special Part, and shall propose, to the Bank's appointed personnel, any improvements or changes to be made should any significant breaches of occupational health and safety regulations emerge, or should there be any changes in

organization or activities following scientific or technological advancements;

b. propose, and cooperate on the preparation of, control procedures concerning the measures to be taken in those risk areas identified in this Special Part, designed to guarantee the safeguarding of occupational health and safety, in keeping with the provisions of this Model and of Section 30 of the Decree on Occupational Health and Safety;
c. examine any reports of alleged infringement of the Model, and carry out the necessary or appropriate checks in relation to any such reports received.

In order to duly perform its duties, the SB may:

- attend the meetings organized by the Bank involving those functions in charge of health and safety, and decide which meetings are of importance for the correct performance of its duties;
- regularly meet the Health and Safety Officer;
- access all documents and all sites of importance for the performance of its duties.

The Bank guarantees to provide the SB with flows of information capable of allowing the latter to acquire the information it requires for the purpose of monitoring accidents, critical issues and news of any confirmed or suspected professional illnesses.

In carry out the aforementioned activities, the SB may avail itself of all of the Bank's competent resources.

Finally, it should be noted that Banca Sistema, with the support of a firm of specialized consultants, has drawn up the Planning Document following Risk Assessment, and thus, if such is applied in full, it may constitute the basis for an organizational and management model capable of exempting the Entity from any administrative liability pursuant to Italian Legislative Decree no. 231/01 and subsequent additions and amendments, provided that the Ethical Code has been drawn up, and the SB appointed complete with its own Regulations and any disciplinary means.