ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL
pursuant to Legislative Decree 231 of 8 June 2001

Approved by the Board of Directors on 29 July 2022

INTESA SANPAOLO

TABLE OF CONTENTS

1.1 The administrative liability scheme laid down in Legislative Decree 231 of 8 June 2001 for legal persons, companies and associations, including those without legal personality.

By way of implementation of the delegation under Article 11 of Law 300 of 29 September 2000, on 8 June 2001 Legislative Decree 231 (hereinafter the "Decree" or "Legislative Decree 231/01") was adopted, aligning national legislation with the international conventions on the liability of legal persons. These are, specifically, the Brussels Convention on the protection of the European Union' financial interests of 26 July 1995, the Convention on the fight against corruption involving officials of the EU or officials of Member States of the European Union, signed in Brussels on 26 May 1997, and the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions of 17 December 1997.

The Decree, which lays down "*Provisions on the administrative liability of legal persons, companies and associations, including those without legal personality*", introduced into the Italian legal order an administrative liability regime applying to Entities (meaning companies, associations, consortia, etc., hereinafter, "Entities") for a series of specified offences committed[1] in the interest or to the advantage of the entity: (i) by natural persons holding representation, administration or management positions in the Entity or in a financially and functionally autonomous organisational unit belonging to the Entity; and by natural persons who exercise, also de facto, the management and control of the Entity, or (ii) by natural persons subject to the management or supervision of one of the above-mentioned persons. The list of "predicate offences" was recently expanded by the addition of some types of administrative breaches.

The Entity's liability is additional to that of the natural person who committed the offence, and is independent of it, as it also exists where the offender has not been identified or cannot be charged or where the offence is extinguished for a reason other than amnesty.

The administrative liability regime laid down in the Decree for prosecution of the offences specifically identified therein, applies to Entities which benefited from the offences or in whose interest the predicate offences - or administrative breaches - identified in the Decree were committed. The penalties applicable to the Entity may include fines, bans, confiscation, publication of the sentence and appointment of a special administrator. Prohibitory measures, which may have a more severe impact on the Entity than monetary penalties, consist in the suspension or revocation of licenses and concessions, prohibition on contracting with the public administration, prohibition on conducting

[1] An entity is also liable for attempted offences i.e. in cases where acts are carried out that are unequivocally intended to commit one of the offences indicated as a predicate offence of the legal entity.

business activities, denial or revocation of funding and contributions, and the prohibition on advertising products and services.

The above-mentioned liability also applies to offences committed abroad, provided that the country in which the offence was committed does not initiate proceedings in respect of those offences and that the Entity has its head office in Italy.

1.2 The adoption of the organisational, management and control models as a means to exempt Entities from administrative liability

After establishing the administrative liability of Entities, in Article 6 the Decree provides that an Entity shall not be liable where it can prove that it *".... adopted and effectively implemented, before the offence was committed, an appropriate organisation and management model to prevent offences of the kind that has occurred...".*

Article 6 also provides for creation of an internal control body within the Entity, tasked with ... *"monitoring the operation, effective implementation and observance of the model..."*, and with updating the model.

The "Organisational, Management and Control Model" adopted in accordance with Legislative Decree 231 of 8 June 2001 (the "Model") has to meet the following requirements:

- identify the activities which may give rise to the offences listed in the Decree;
- define the procedures through which the entity makes and implements decisions relating to the offences to be prevented;
- define procedures for managing financial resources to prevent offences from being committed;
- establish reporting obligations to the body responsible for monitoring Model operation and compliance;
- put in place an effective disciplinary system to punish non-compliance with the measures required by the Model.

If the offence is committed by persons holding a representative, administrative or management role in the Entity or one of its organisational units with financial and functional autonomy and by persons who, de facto or otherwise, manage and control the Entity, the Entity shall not be liable if it can prove that:

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

On the other hand, where the offence is committed by persons under the management or supervision of one of the above-mentioned persons, the Entity is liable if perpetration of the offence was made possible by non-performance of management and supervisory duties. Such non-performance shall be ruled out where the Entity, before the offence was committed, had adopted and effectively implemented an appropriate Model to prevent offences of the kind committed, based, of course, on a priori assessment.

Lastly, Article 6 of the Decree provides that the Model may be adopted on the basis of codes of conduct prepared by representative trade associations and submitted to the Ministry of Justice.

The Model of Intesa Sanpaolo S.p.A. (the “Bank” or “Parent Company”) was prepared and updated also having regard to the guidelines prepared by ABI and approved by the Ministry of Justice.

CHAPTER 2 THE ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL OF INTESA SANPAOLO S.P.A.

2.1 The existing corporate tools underlying the Model

2.1.1 Introduction

In preparing this Model, account was taken firstly of the current legislation and of the procedures and control systems already existing and implemented within Intesa Sanpaolo S.p.A., insofar as they were appropriate to also serve as measures for preventing offences and unlawful conduct in general, including those laid down in Legislative Decree 231/01.

Intesa Sanpaolo S.p.A. is a highly complex reality, from both the organisational and operational viewpoint. The corporate bodies of Intesa Sanpaolo S.p.A. have given the highest importance to aligning the organisational structures and operational procedures both to ensure efficiency, effectiveness and transparency in the management of activities and the associated allocation of responsibilities, and to minimise any inefficiencies, failures and irregularities (including any conduct which is unlawful or otherwise not in line with Bank guidelines).

The organisational context of Intesa Sanpaolo S.p.A. consists of the corpus of rules, structures and procedures which ensure the Bank's operation; it is therefore a multifaceted system which is defined and checked internally also with a view to compliance with the legislation applicable to Intesa Sanpaolo S.p.A. as both a bank and a listed company (Banking Law, the Consolidated Law on Financial Intermediation, etc.) and consequential provisions issued by the Supervisory Authorities, European Central Bank, Bank of Italy, Consob etc., within their respective powers, which carry out checks and controls on the Bank's activities and organisational structure, as provided for by law.

Also, the Intesa Sanpaolo Group, pursuant to Legislative Decree 254/2016, is required to prepare and publish, to the extent necessary to ensure a clear understanding of the Group's activities and the impacts thereof, its performance and results, a consolidated non-financial statement that covers topics ranging from the environment, social issues, matters related to personnel, the respect for human rights to the fight against passive and active bribery. The Statement must describe the company's management and organisational business model, including the organisational and management models adopted pursuant to Legislative Decree 231/2001, including with regard to the management of the aforementioned topics and the principal risks that arise from them.

Clearly, therefore, this corpus of special rules, together with ongoing supervision by the competent Authorities constitute invaluable tools for preventing unlawful conduct in general, including the offences laid down in the specific legislation on the administrative liability of Entities.

The Bank's already existing specific tools laying down the procedures through which the entity makes and implements decisions relating to the offences and breaches to be prevented include:

- the rules of corporate governance adopted in accordance with the Corporate Governance Code for listed companies and the relevant corporate laws and regulations;
- internal regulations and corporate policies;
- the Group's Code of Ethics, Internal Code of Conduct and Anti-corruption Guidelines;
- the internal control system;
- the powers and delegation system.

The rules, procedures and principles set out in the above-mentioned instruments are not described in detail in this Model but are integrated in the Model's broader organisational, management and control system which all internal and external parties are required to respect, in accordance with their relationship with the Bank.

The following paragraphs provide an overview of the reference principles of the Group's Code of Ethics, Internal Code of Conduct and Anti-corruption Guidelines, the internal control system, and the powers and delegation system.

2.1.2 The Group's Code of Ethics, Internal Code of Conduct and Anti-corruption Guidelines

In line with the importance assigned to ethical issues and to pursuing a conduct consistently inspired by criteria of rigour and integrity, the Bank has adopted a Group-wide Code of Ethics, an Internal Code of Conduct and Anti-corruption Guidelines.

The Code of Ethics is a voluntary, self-regulating tool that is an integral part of the Sustainability management model. It contains the mission, corporate values and the principles that regulate the relationships with the stakeholders, starting with the corporate identity. In certain particularly relevant areas (i.e. human rights, employment protection, environmental protection, the fight against corruption) the Code refers to rules and principles that are consistent with the best international standards.

The Group's Internal Code of Conduct, applicable to all Group Companies, is an intentionally lean set of rules. It includes general provisions – defining the essential rules of conduct for company representatives, staff and external collaborators who, in performing their duties, must operate with professionalism, diligence, honesty and correctness – and more specific provisions, such as the prohibition to engage in certain personal transactions.

With best international practices, the Anti-corruption Guidelines identify the principles, sensitive areas and define the Group's roles, responsibilities and the macro-processes for handling of the risk of corruption. They also provide for the Anti-Money Laundering function to undertake responsibility for governing this area and the Head of this department shall be the Head of Corporate Anti-corruption.

2.1.3 The key features of the internal control system

Intesa Sanpaolo S.p.A., to ensure sound and prudent management, combines business profitability with an attentive risk-acceptance activity and an operating conduct based on fairness.

Therefore, the Bank, in line with legal and supervisory regulations in force and consistently with the Code of conduct of listed companies, has adopted an internal control system capable of identifying, measuring and continuously monitoring the risks typical of its business activities.

Intesa Sanpaolo S.p.A.'s internal control system is built around a set of rules, procedures and organisational structures aimed at ensuring compliance with Company strategies and the achievement of the following objectives:

- the effectiveness and efficiency of Company processes;
- the safeguarding of asset value and protection from losses;
- the reliability and integrity of accounting and management information;
- transaction compliance with the law, supervisory regulations as well as policies, plans, procedures and internal regulations.

The internal control system is characterised by a documentary infrastructure (regulatory framework) that provides organised and systematic access to the guidelines, procedures, organisational structures, and risks and controls within the business, incorporating both the Company policies and the instructions of the Supervisory Authorities, and the provisions of the law, including the principles laid down in Legislative Decree 231/01.

The regulatory framework consists of "*Governance Documents*" as adopted from time to time, which oversee the operation of the Bank (Articles of Association, Code of Ethics, Group Internal Code of Conduct, Group Committee Regulations, Regulation on Related Party Transactions, Regulations regarding the integrated internal control system, Authorities and powers, Guidelines, Function/Organisational Charts, Organisational Models, etc.) and of more strictly operational regulations that govern business processes, individual operations and the associated controls (Rules, Process Guides, Control Sheets, etc.).

More specifically, the Company rules set out organisational solutions that:

- ensure sufficient separation between the operational and control functions and prevent situations of conflict of interest in the assignment of responsibilities;
- are capable of adequately identifying, measuring and monitoring the main risks assumed in the various operational segments;
- enable the recording of every operational event and, in particular, of every transaction, with an adequate level of detail, ensuring their correct allocation over time;
- establish reliable information systems and suitable reporting procedures for the various management levels having control functions;

- ensure prompt reporting to the appropriate levels within the company and the swift handling of any anomalies found by the business units, by the Internal Auditing function or by other control functions.

Moreover, the Company's organisational solutions provide for control activities at all operational levels, which make it possible to identify responsibilities univocally and formally, in particular as concerns performing controls and correcting any irregularities found.

Following the indications provided by the Supervisory Authorities, the Bank has identified the following types of control described in detail within the Integrated Internal Control System Regulations:

- ***first level***: line controls that aim to ensure correct application of the operations (e.g. hierarchical, systemic controls or controls on a sampling basis) which are, to the extent that is feasible, incorporated in IT procedures. These activities are carried out by the same operating and business structures, including through units dedicated exclusively to control functions, which report to the managers of the structures themselves, or they are executed within the back office. The operating and business structures are the first line responsible parties for the risk management process and are required to comply with the operating limits assigned to them consistently with the risk objectives and the procedures which comprise the risk management process;
- ***second level***: controls on risks and compliance that aim to ensure among other things: i) correct implementation of the risk management process, ii) compliance with the operating limits assigned to the various functions, iii) compliance of corporate operations with the laws, including self regulation. The functions in charge of these controls are distinguished from the production functions and they participate in defining the risk and governance policies and the risk management process;
- **third level:** internal auditing, aimed at identifying violations of procedures and regulations, as well as periodically assessing completeness, adequacy, functionality (in terms of efficiency and effectiveness) and the reliability of the internal control systems and the information system at pre-set intervals depending on the nature and intensity of the risks. It is performed by different structures which are independent from production structures.

The internal control system is periodically reviewed and adapted in relation to business developments and the reference context.

In particular, the internal audit activities in Intesa Sanpaolo S.p.A. are carried out by the Internal Auditing function, which reports directly to the Board of Directors (and the Chair thereof), which functionally reports to the Management Control Committee, notwithstanding the appropriate interchanges with the Managing Director and CEO. This function is also tasked with submitting to the Board of Directors, the Management Control Committee, the Top Management and the Heads of the various Organisational units, proposals for possible improvements to risk management policies, measurement tools, processes and procedures.

2.1.4 The powers and delegation system

Under the Articles of Association, the Board of Directors is vested with all the powers for the ordinary and extraordinary administration of the Bank.
The Board of Directors has delegated some of its functions to the Managing Director and C.E.O in order to ensure consistency of current management, in implementation of the Board resolutions. The Board of Directors has also defined and approved the decision-making powers and expenditure limits of the Heads of the Organisational Structures, in accordance with the organisational and management responsibilities assigned to them, setting the limits thereof and establishing procedures and limits for exercise of sub-delegations.
The power to sub-delegate is exercised through a constantly monitored transparent process, which is calibrated in accordance with the role and position of the sub-delegate, who in any case must report back to the delegating function.
Moreover, the procedures for signing deeds, contracts, documents and internal and external correspondence are formalised, and the relevant signing powers are assigned to staff members jointly or severally. In particular, joint signatures are usually required for documents issuing orders or accepting obligations for the Bank.
All the Structures operate under specific Regulations defining their powers and responsibilities; these regulations are issued by and notified within the Bank. The document on autonomous management powers, approved by the Board of Directors, is also disseminated throughout the Bank.
Lastly, operational procedures, which define how the different corporate processes are to be performed are also disseminated throughout the Bank by means of specific internal rules.
Therefore, all the main decision-making and implementing processes concerning Bank operations are spelled out, observable and available to the entire organisation.

2.2 The aims pursued by the model

Although the corporate tools described in the preceding paragraphs would by themselves suffice to prevent the offences covered by the Decree, the Bank decided to adopt a specific Organisational, Management and Control Model pursuant to the Decree, convinced that such model, besides being an important tool for raising the awareness of all those who operate on the Bank's behalf, leading them to operate with integrity and transparency, is also more effective in preventing the risk of the offences and the administrative breaches covered by the reference legislation being committed.
In particular, by adopting and regularly updating the Model, the Bank pursues the following main aims:

- make all persons operating on the Bank's account in the field of "sensitive activities" (i.e. those activities which, by their nature, are at risk for the offences identified in the Decree), aware of the fact that, should they breach the rules governing such activities, they might incur disciplinary and/or contractual sanctions, as well as criminal and administrative penalties;
- stress that any such unlawful conduct is strongly discouraged since (even where the Bank would seem to benefit from it) such behaviour is in breach not only of the law, but also of the ethical principles which the Bank intends to apply to all its activities;
- enable the Bank, thanks to monitoring of the sensitive activity areas, to take swift action to prevent or fight any offences and punish conduct in breach of its Model.

2.3 Key model components

The key model components may be summarised as follows:

- identification of the activity areas at risk, i.e. the sensitive company activities where offences might occur, to be analysed and monitored;
- management of operational processes ensuring:
  - the separation of duties by adequately allocating responsibilities and establishing appropriate authorization levels in order to avoid functional overlaps or operating allocations that concentrate activities on a single person;
  - clear and formalised allocation of powers and responsibilities, expressly indicating the limits of those powers and consistent with the duties assigned and positions covered within the organisational structure;
  - appropriate procedures for performing the activities;
  - traceability of the acts, operations and transactions through an appropriate paper or electronic trail;
  - decision-making processes linked to previously established objective criteria (e.g.: the company keeps registers of approved suppliers, objective staff assessment and selection criteria are in place, etc.);
  - control and supervisory activities on company transactions are in place and traceable;
  - safety mechanisms are in place, providing appropriate data protection/access control to corporate data and assets;
- adequate rules of conduct are in place ensuring that corporate activities are carried out in compliance with the laws and regulations and safeguarding the company's assets;
- the responsibilities for the adoption, amendment, implementation and control of the Model have been defined;
- the Surveillance Body has been identified and specific duties of oversight on the Model's effective and proper functioning have been allocated;
- the information flows to the Surveillance Body have been defined;
- an effective disciplinary system has been put in place and implemented to punish non-compliance with the measures required by the Model;

- staff training and internal communication concerning the contents of the Decree and of the Model, and the associated compliance obligations.

2.4 Model structure

To define this "*Organisational, Management and Control Model pursuant to Legislative Decree 231 of 8 June 2001*" Intesa Sanpaolo S.p.A., the company that resulted from the merger by incorporation of Intesa S.p.A. and Sanpaolo IMI S.p.A., adopted an approach based on the internal rules and procedures already in place in the aforementioned companies, which were supplemented, thereby making the most of the experience already gained by the two Banks.

Based on the structure of the Bank post merger, "sensitive" corporate areas have been identified for each category of "predicate offence". Within each sensitive area the corporate activities most at risk for the perpetration of the predicate offences laid down in the Decree ("sensitive" activities) have been identified, and for each of such activities conduct and control rules have been established – differentiated according to the specific offence-risk to be prevented.

The Model is fully and effectively implemented in the Bank's operations by connecting each sensitive area with the corporate structures concerned from time to time and with the dynamic management of processes and of the reference internal regulations, which must be based on the conduct and control principles spelled out for each such activity.

The approach adopted:

- helps make optimum use of the Bank's store of knowledge concerning the internal policies, rules and regulations guiding and governing its decision-making and implementation concerning the prevention of unlawful acts, and, more in general, risk management and the performance of controls;
- makes it possible to manage the corporate operating rules with univocal criteria, including those relating to "sensitive" areas;
- facilitates the continual implementation and prompt alignment of processes and internal regulations with changes in the organisational structure and company operations, ensuring a considerable level of "dynamism" of the model.

Accordingly, the control of the risks under Legislative Decree 231/2001 by the Bank is ensured by:

- this document ("Organisational*, Management and Control Model*");
- the existing regulatory system, which is an integral and substantive part of this model.

The "*Organisational, Management and Control Model*" sets out in particular:

- the reference regulatory framework;

- the roles and responsibilities of the structures engaged in the adoption, effective implementation and modification of the model;
- the specific duties and responsibilities of the Surveillance Body;
- the information flows to and from the Surveillance Body;
- the system of sanctions;
- the training principles;
- the "sensitive" areas having regard to the types of offences identified in the Decree;
- the corporate activities at risk for the predicate offences ("sensitive" activities) and the rules of conduct and controls aimed at preventing such offences.

The Bank's regulatory framework of the Bank, consisting of the "*Governance Documents*" (Articles of Association, Code of Ethics, Group Internal Code of Conduct, Regulations, Guidelines, Powers, Organizational Structure Function Charts, etc.), and Rules, Process Guides, Control Sheets and other tools, governs at the various levels the Bank's operations in the sensitive areas/activities and is for all intents and purpose an integral part of the Model.

The regulatory framework is held and catalogued, with specific reference to each "sensitive" activity, in a specific document repository, which is available throughout the Bank through the company's Intranet and constantly updated by the competent functions in line with the development of the operations.

Therefore, by matching the contents of the Model with the corporate regulatory framework it is possible to extract, for each of the "sensitive" activities, specific, precise and always up-to date Protocols that set out phases of activities, the structures concerned, control and conduct principles, and process operating rules and which make it possible to verify and streamline each activity phase.

2.5 The addressees of the Model

The Model and the provisions it contains or refers to must be complied with by all the managers and staff of Intesa Sanpaolo S.p.A. (including those recruited and/or working abroad) and, in particular, by those who perform sensitive activities.

Staff training and the dissemination of information on Model contents within the organisation are continuously ensured by the procedures described in detail in Chapter 6 below.

In order to ensure the effective and efficient prevention of offences, the Model is also addressed to external stakeholders (i.e. suppliers, agents, consultants, professionals, self-employed or "para-subordinate" workers, commercial partners or other individuals) who, under contractual relationships, collaborate with the Bank in performance of its activities. Their compliance with the Model is ensured by a contractual clause whereby they undertake to comply with the principles of the Model and the Anti-Corruption Guidelines and to report to the Surveillance Body and the Anti-Corruption Officer any

offences or violations of the Model. The violation of obligations or other offences that may be committed during or in relation to their duties will to all intents and purposes constitute a serious violation within the meaning of article 1455 civil code for the purposes of termination of the contract.

2.6 Model adoption, effective implementation and modification – Roles and responsibilities

Adoption of the Model

In accordance with Article 6, paragraph I, point (a) of the Decree, the *"Model"* is adopted by resolution of the Board of Directors, which also supervises its implementation, upon receiving the opinion of the Surveillance Body.

To this end, the Managing Director and C.E.O. submits for the Board of Directors' approval the Model, drafted with the assistance of the relevant departments, within their respective remits (Compliance, Internal Auditing, Legal Affairs, Organisation, Process Management and Development, Human Resources, Anti-Money Laundering functions, Employer and Principal pursuant to Legislative Decree 81/08 "*Implementation of Article 1 of Law 123 of 3 August 2007 on health and safety in the workplace*" - hereinafter: Legislative Decree 81/08, Environmental Affairs Officer pursuant to Legislative Decree 152/2006).

Effective implementation and modification of the Model

The Board of Directors (or the entity formally delegated by it) is tasked with effectively implementing the Model, by assessing and approving the actions required to implement or amend it. In identifying such actions, the Board of Directors is assisted by the Surveillance Body.

The Board of Directors delegates the individual structures to implement Model contents and to regularly update and implement the internal regulations and corporate processes, which are an integral part of the Model, in compliance with the control and conduct principles defined for each sensitive activity. Effective and concrete Model implementation is also ensured:

- by the Surveillance Body, in the exercise of its powers of initiative and control over the activities carried out by the individual organisational units in the sensitive areas;
- by the heads of the Bank's various Organisational units (Governance Areas, Divisions, Departments and Organisational units) having regard to the activities at risk they perform.

The Board of Directors, also with the help of the Surveillance Body, must also ensure updating of the sensitive areas and of the Model, in view of any adaptations that may be necessary.

Specific roles and responsibilities relating to Model management are also assigned to the functions indicated below.

Internal Auditing function

Internal Auditing delivers ongoing and independent surveillance on the regular performance of operations and processes, in order to prevent or detect any anomalous or risky behaviour or situation. It assesses the efficiency of the overall internal control system and its ability to guarantee effective and efficient company processes.

This function supports the Surveillance Body in monitoring compliance with and adequacy of the rules contained in the Model. Whenever problems are identified, it refers them to the competent functions for the appropriate mitigation actions.

Compliance function

The task of the Compliance function is to ensure consistently over time that effective rules, procedures and operational practices are in place to prevent breaches or violations of applicable provisions.

With specific reference to the administrative liability risks introduced by the Decree, the Compliance function supports the Surveillance Body's performance of its control activities by:

- defining and updating the Model, with the support of Legal, Organisation, Process Management and Development, in line with developments in the reference legislation and with changes in both the Employer's and the Principal's organisational structure, under Legislative Decree 81/08, of the Environmental Affairs Officer pursuant to Legislative Decree 152/2006), as well as of the Anti-Money Laundering function - each as to their respective areas of competence;
- monitoring, over time, Model effectiveness with reference to the rules and principles of conduct for the prevention of sensitive offences; to this end the Compliance function:
  - identifies each year those processes felt to be at higher risk both as to their contents with respect to the predicate offences, and as to the existence or non-existence of specific procedures to mitigate such risk; once the processes have been identified and before they are published on the company's system of regulations, the compliance function issues a preliminary approval as to the correct application of the control and conduct principles provided for by the Model; moreover, by means of a risk-based approach, it implements specific assurance activities to assess the conformity of the processes with the "protocols" set out in the Model;
  - analyses the results of the organisational units' self-assessment process and statement on compliance with the control and conduct principles set out in the Model;
- examining the information submitted by Internal Auditing on issued detected during its verifications.

Anti-Money Laundering function

The Anti-Money Laundering function constantly checks that the company's procedures are consistent with the aim of preventing and combating the violation of external regulatory requirements (laws and regulations) and self-regulation on the subject of money laundering, terrorism financing, the violation of embargoes and weapons and anti-corruption legislation.

To pursue the aims set out in the Decree, the Anti-Money Laundering function, exclusively with regard to managing risks inherent to anti-money laundering, terrorism financing, embargoes and weapons and anti-corruption legislation:

- contributes to the definition of the Model's structure and to its update;
- promotes organisational and procedural amendments aimed at ensuring an adequate monitoring of the risks inherent to money laundering and terrorism financing;
- receives and forwards the periodical reports and the information flows set out in the "*Guidelines for contrasting money laundering and terrorism financing phenomena and for managing embargoes*";
- sets up, in co-operation with the company structures responsible for training, adequate training activities aimed at keeping employees and collaborators constantly updated.

Legal Affairs function

Legal Affairs pursues the aims set out in the Decree by providing assistance and legal advice to the Bank's structures, monitoring the development of the relevant legislation and case law.

Other tasks of the Legal Affairs function are to interpret the legislation, resolve legal issues and identify types of conduct which may constitute offences.

Legal Affairs collaborates with the Compliance, Internal Auditing, Organisation, Process Management and Governance and Anti-Money Laundering functions, with the Employer and the Principal pursuant to Legislative Decree no. 81/2008 and with the Environmental Affairs Officer pursuant to Legislative Decree 152/2006, in updating the Model, also reporting any widening of the scope of the administrative liability of Entities.

Organisation, Process Management and Development functions

The duty of the Organisation, Process Management and Development functions, within the scope of their respective competences, is to ensure that the organisational structure and governance mechanisms are in line with the objectives pursued by the Model. Accordingly, they shall:

- design the organisational structure, defining its missions, organisation charts and functions, and submits it for approval to the Managing Director and CEO;
- define the rules for the design, official adoption and management of the organisational processes;
- support the design of the organisational processes or validate procedures defined by other functions, ensuring their consistency with the overall organisational plan;

- identify, for each sensitive company process, the main Organisational Unit responsible tasked with self-assessment and reporting to the Surveillance Body;
- work with the business units, Internal Auditing, Compliance and Legal Affairs, Anti-Money Laundering, the Employer and with the Principal pursuant to Legislative Decree 81/08, with the Environmental Affairs Officer pursuant to Legislative Decree 152/2006, and with the other corporate functions concerned, each within its sphere of competence, in updating the regulatory system and the Model (following changes to the applicable legislation or in the company's organisational setup and/or operating procedures, relevant for the purpose of the Decree);
- disseminate the internal rules throughout the Bank's organisation through the company's Intranet.

Human Resources Function

The Human Resources function, as detailed in chapter 5 and chapter 6:

- develops training plans and awareness-raising actions, with support from the competent functions and the Training and Internal Communications functions, addressed to all staff members concerning the importance of adhering to the company's rules of conduct, understanding the contents of the Group's Model, Code of Ethics, Internal Code of Conduct and Anti-corruption Guidelines and specific courses addressed to the staff operating in the sensitive areas, in order to clarify in detail issues, early warning signs of anomalies or irregularities and the mitigation actions to be taken for anomalous or risk-exposed operations;
- manages, with support from the Compliance, Internal Auditing, Anti-Money Laundering and Legal Affairs functions, the process of detecting and handling any non-compliance with the Model, and the consequent system of penalties; they also report all information collected concerning the facts and/or conduct relevant to compliance with the provisions of the Decree to the Surveillance Body, which analyses it in order to prevent future breaches and monitor Model adequacy.

Organisational Units

The Organisational units are tasked with the execution, proper functioning and sustained effective process application over time. The internal regulations identify the Organisational Units tasked with designing the processes.

For the specific purposes of the Decree, the Organisational units have a duty to:

- review – in the light of the rules of conduct and principles applicable to sensitive activities - the practices and processes falling under their remit, to make them suitable to prevent unlawful conduct;
- report to the Surveillance Body any cases of irregularities or anomalous conduct.

In particular, the above-mentioned Organisational units for sensitive company activities should pay the highest and constant care in verifying the existence of and remedying any shortcomings in the regulations or procedures which may give rise to foreseeable risks of "predicate offences" being committed within the activities under their remit.

Employer and Principal pursuant to Legislative Decree 81/08, Environmental Affairs Officer pursuant to Legislative Decree 152/2006

The parties identified as Employer and Principal pursuant to Legislative Decree 81/08, and Environmental Affairs Officer pursuant to Legislative Decree 152/2006, only as concerns their respective area of responsibility for managing the risks relating to the environment, workplace health and safety and to temporary or mobile construction sites shall:

- participate in defining the model's structure and in its updating;
- identify and assess the emergence of risk factors for predicate offences;
- promote organisational and procedural changes aimed at adequately controlling non-compliance risk.

2.7 Outsourced activities

The Model of Intesa Sanpaolo S.p.A. provides for the outsourcing of company operations, or parts of them, to other Group companies and/or to external outsourcers. In particular, the Bank has assigned, among others, credit recovery activities for non-performing and bad loans, including those arising from financial leases, cash management, the design and production of training services and products, use of IT cloud solutions and management of payment cards and ATM withdrawals to external outsourcers.

Outsourcing of the activities is carried out in accordance with the prescriptions of the Supervisory authorities and is formalised through the conclusion of specific contracts that enable Intesa Sanpaolo S.p.A. to:

- take all decisions by exercising its autonomy, as it maintains the necessary competences and responsibilities on the activities relating to the outsourced services;
- consequently maintain guidance and control powers on the outsourced activities.

In particular, these contracts envisage, in compliance with current legislation on outsourcing, specific contractual clauses including:

- the outsourced activities in detail;
- the procedures for providing the services;
- the specific service levels;
- the verification and control powers remaining with the Bank;
- the procedures for setting rates for the services provided;
- suitable reporting systems;
- appropriate safeguards protecting the Bank's information assets and transaction security;

- the obligation of the outsourcer to operate in compliance with applicable laws and regulations, and to ensure that third parties appointed to carry out outsourced activities observe said laws and regulations;
- the possibility for Intesa Sanpaolo S.p.A. to terminate the contract in the event the outsourcer violates: (i) the laws and directives from the Supervisory Authorities that may result in penalties imposed on the principal; (ii) the obligation to implement activities in compliance with the principles laid down in the *Organisational, Management and Control Model* pursuant to Legislative Decree 231 of 8 June 2001 adopted by Intesa Sanpaolo S.p.A. and with the Group's Code of Ethics, Internal Code of Conduct, and Anti-corruption Guidelines.

Dedicated Bank structures shall constantly verify, also through control of the required service levels, compliance with contractual clauses, hence adequacy of the activities performed by the service provider.

2.8 Models of the companies belonging to the Banking Group

Without prejudice to the independent responsibility of each Intesa Sanpaolo Group company as regards the adoption and efficient implementation of their own *Model* in accordance with the Decree, in exercising its specific function as Parent Company, the Bank has the power to establish criteria and guidelines of a general nature and to verify, through the Compliance, Internal Auditing and M&A and Group Investments functions, whether the Models of Group companies comply with such criteria and guidelines.

2.8.1 Group guidelines concerning the administrative liability of Entities

In order to harmonise at Group level the procedures for transposing and implementing the contents of the Decree by putting in place appropriate risk control procedures, we outline below the guidance principles which all the companies incorporated in Italy are required to comply with, in accordance with their legal autonomy and with the principles of sound corporate management.
In particular, each company concerned shall:

- adopt its own Model, after identifying the corporate activities at risk for the offences provided for by the Decree and the measures best able to prevent such offences. In preparing the Model, the company shall follow the principles and contents of the Parent Company's Model, except where there are specific situations relating to the nature, size or type activity pursued or the company's

structure, the organisation and/or the allocation of internal delegations making it necessary or advisable to adopt different measures in order to pursue the Model's objectives more effectively, while always respecting the above-mentioned principles and those laid down in the Code of Ethics and in the Group's Internal Code of Conduct and Anti-corruption Guidelines. In the case of substantial discrepancies with the principles and contents of the Model of Parent Company, the Parent Company's Compliance function shall be informed of the reasons for such differences, and shall receive the final draft of the Model prior to its approval by the Corporate governance bodies. The company shall inform the Compliance function of having adopted the Model by sending a copy thereof and the Board of Directors' approval resolution. Pending approval of the Model, the company shall adopt all appropriate means to prevent unlawful conduct;

- promptly appoint the Surveillance Body, in line with the Parent Company's recommendations on the persons to be appointed. The Compliance, M&A and Investments functions of Intesa Sanpaolo S.p.A. are informed of the nomination. If the members of the Surveillance Body are not the same as those of the subsidiary's control body, the Management Control Committee must be provided with specific information in the report on activities overseen by the Surveillance Body;
- ensure systematic Model updating as required by legislative and organisational changes, or where significant and/or repeated breaches of the rules of the Model make it necessary. Any legislative amendments shall be notified by a specific communication to be sent to the company by the Parent Company's Compliance function. Confirmation of the Model having been updated shall be provided to the Compliance function following the procedures described above;
- provide training and communication activities for all staff, in collaboration with the Parent Company Personnel and Compliance functions and with support from the Training and Internal Communications functions, as well as specific training for roles engaged in activities that are more "sensitive" (see Legislative Decree 231/01) – including officers shared with the Parent Company - in order to create widespread awareness and a strong corporate culture in this field;
- adopt appropriate controls of the processes which are "sensitive" with respect to the Decree, covering their identification, documentation and publication within the corporate regulatory system. Moreover, processes considered most at risk based on qualitative considerations regarding predicate crimes, and whether specific controls exist to mitigate relative risk, must be identified annually, by the company compliance function, or if not present, by the function specifically identified to monitor the administrative liability of entities. For these processes, the compliance function:
  - issues a preliminary approval, prior to their publication, concerning the sound application of the control and conduct principles provided for by the Model;
  - implements specific assurance activities to assess the conformity of the processes with the "protocols" set out in the Model;
- performs, once a year, a self-assessment review of the activities carried out to verify the degree of Model *implementation*, with special regard to compliance with control and conduct principles and with operating rules. The self-assessment review shall be initiated in coordination with the Parent Company's Risk Management and Compliance functions;
- gives the Parent Company Compliance function a copy of periodic reports, including the results of the self-diagnostic process, presented by the compliance function to the Surveillance Body.

The company's Surveillance Body shall also forward to the Parent Company Management Control Committee and Surveillance Board, through the secretarial team, the periodic report, drawn up as a rule every six months, on the activity performed and submitted to the Board of Directors, together with any remarks made by such Board.
Information flows can also be provided between the Surveillance Body of the Parent Company and the Bodies of the companies - also through training meetings on topics of common interest - in order to enable the coordination of the Group's Surveillance Bodies and a better and more effective supervision of preventive measures within the individual corporate entities.
With regard to the above-mentioned activities, the competent Parent Company functions shall, within their respective spheres of competence, support and assist the companies in performing their duties.

In accordance with the Group-wide compliance guidelines, for the specifically named companies[2], whose operations are highly integrated with the Parent Company's, the compliance controls concerning the administrative liability of Entities shall be handled centrally by the Parent Company's compliance function; nevertheless, the competence and responsibility to approve and effectively implement the Model and appoint the Surveillance Body shall remain with the companies. Such companies are responsible for the following activities:

- handling of the Model formalisation and approval process by the competent Corporate governance bodies;
- support the Parent Company in collecting the information necessary to identify the company's specific sensitive areas and activities;
- file and store the documentation concerning the outcomes of the self-assessment and of the reports to the Corporate governance bodies;
- forward to the Parent Company's Compliance function a copy of the notices convening the meetings of the Surveillance Body and the meetings of the Corporate governance bodies whenever Decree-related issues are on the agenda.

[2] Under outsourcing agreements/contracts.

CHAPTER 3 THE SURVEILLANCE BODY (SB)

3.1 Composition and duties of the Surveillance Body

The task of continuously monitoring effective implementation of the Model, ensuring observance and proposing updates to improve the efficacy of crime and unlawful acts prevention pursuant to Article 6 of Legislative Decree 231/01, which is entrusted to the Surveillance Body, a body within the Entity with autonomous powers of initiative and control.

In consideration of the governance structure adopted by the Bank and the size and complexity of its structure, the functions of the Surveillance Body are assigned to a board comprised of three members who are external to the Bank, in order to ensure autonomy, independence, professionalism and integrity in the exercise of its duties.

To this end and pursuant to Legislative Decree 231/01, the Surveillance Body exclusively supervises implementation and observance of the Model by the individuals reporting to it and formulates proposals for the amendment thereof, to improve its efficacy as to the prevention of the crimes included in the list contained within Legislative Decree 231/01.

3.2 Autonomy of the Body

The Surveillance Body has powers of initiative and control over the activities of the Bank. It is not vested with management powers.

In order to allow it to exercise its functions with complete independence, the Surveillance Body is attributed its own annual budget, which is approved by the Board of Directors, upon the favourable opinion of the Body itself.

In order to ensure that the powers of initiative and control are exercised autonomously towards all persons who are subject to the rules which are set forth or referred to in the Model, the Surveillance Board may exceed the budget set and approved by the Board of Directors pursuant to the preceding paragraph in exceptional cases of urgency, without requiring prior authorisation. In such cases, the Body must appropriately justify in its minutes the expense and existence of the urgency requirements and obtain ratification by the Board of Directors at the latter’s next meeting.

The operation of the SB is governed by a Regulation of the activities and duties conferred upon it (determination of the frequency of its meetings and audits, convocation and meeting procedures, identification of the criteria and procedures for analysis, appointment of the Chair, etc.).

3.3 Constitution, appointment, duration and remuneration of the Surveillance Body

3.3.1 Constitution and appointment

The Surveillance Body consists of three standing members and three alternate members; the latter take over the exercise of their functions only in the cases provided for by section 3.6.

The Board of Directors constitutes the Surveillance Body, appointing the standing and alternate members from among individuals external to the Bank who fulfil the requirements specified under section 3.4.

Pursuant to the provisions of the Regulation, the Surveillance Body shall appoint a Chair whose duty is to call and chair the Body's meetings.

In the event of revocation, forfeiture or other causes of termination of one or more members, the Board of Directors shall replace the other standing members in compliance with the specialisation criterion and the eligibility requirements set forth under paragraph 3.4.

Members appointed as alternates shall remain in office until expiration of the Surveillance Body's term, as indicated under paragraph 3.3.2.

3.3.2 Duration

The Surveillance Body shall remain in office for the period established by the Board of Directors on appointing it; where no term of office is so specified, the Body shall remain in office until the end of the mandate of the Board of Directors that appointed it; in any case its mandate ends from the time the new Body is re-elected.

3.3.3 Compensation

The Board of Directors, after receiving the recommendations of the Remuneration Committee shall establish the remuneration for the entire term of office of the members of the Surveillance Body for performance of their duties, and those of the alternate members, in the form of a fixed sum for each participation in meetings.

Standing and alternate members shall also receive reimbursement of documented expenses incurred for participation in the meetings.

3.4 Eligibility requirements

The members of the Surveillance Body must meet the professional, independence and integrity requirements specified below.

To this end, interested parties shall submit a specific affidavit to the Board of Directors and provide the specific proof of possession thereof.

3.4.1 Professionalism

a) Members of the Surveillance Body shall possess the same professional requirements as set forth under the Articles of Association (Article 13.5.3, paragraph 1) for Members of the Management Control Committee must have proven experience of at least five years in the areas of internal control, administration and finance gained in the following manners:
   - *i)* as members of the corporate bodies or after having held managerial positions in banking or financial entities with assets of at least 5 billion euro or in insurance entities with gross annual premiums collected of at least 1 billion euro, or entities and companies with revenues of at least 500 million euro (the figures refer to the latest annual results as per the company's financial statements or, if drafted by the entity itself, the consolidated financial statements) or
   - *ii)* through teaching economic or legal course at the university level, which refer in particular to the banking, insurance and financial sector, or
   - *iii)* through the ongoing provision of professional activities or services of a significant level as compared to the typical duties of a control body of the entities and companies indicated under i) above or
   - *iv)* having served as representatives or managers in significant public administrations at least at the regional level or Authorities involved with banking, financial or insurance activities.

b) The members must also have acquired specific, proven experience of at least five years in criminal law or corporate law or business organisation and administrative responsibility of entities, through (as a non-exhaustive example) professional activities or as members of Surveillance bodies of entities which are significant in terms of economic value, legal complexity or size, or through teaching of the above mentioned subjects at the university level.

3.4.2 Independence

The members of the Surveillance Body must fulfil the requirements of independence as set forth under Article 148, paragraph three of Legislative Decree 58/98; at least two members must also fulfil

the requirements of independence as set forth under Article 2 of the Corporate Governance Code and Ministerial Decree 169/2020[3].

3.4.3 Integrity, reputation and fairness

The members of the Surveillance Body must fulfil the requirements of integrity and the reputation and fairness criteria as set forth in current laws applicable to members of the Board of Directors and the Management Control Committee[4].

In any case, nobody can be a member of the Surveillance Body if:

i) they have a non-appealable conviction, even if conditionally suspended (subject to the effects of rehabilitation) for one of the following offences: offences governed by Decree 231/0101, offences concerning corporate failure or insolvency[5]; tax offences.

ii) A sentence is considered to be equivalent to a conviction pursuant to Article 444 of the Code of Criminal Procedure, save for judicial extinction of the offence pursuant to Article 445, paragraph 2 of the Code of Criminal Procedure;

iii) having been a member of the Surveillance Body in companies which have received, by final measure (including the ruling issued pursuant to Article 63 of the Decree), the sanctions laid down in Article 9 of the same Decree, concerning unlawful acts attributed to the entity, committed during their term of office.

3.5 Grounds for disqualification from office

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

i) one of the professionalism, independence and integrity requirements or reputation and fairness criteria needed for eligibility pursuant to article 3.4 above no longer applies; the occurrence of one or more of the situations detailed by art. 4 of the Ministerial Decree 169/2020 regarding the reputation and fairness criteria, or one or more of the situations relevant to the independence requirements, does not automatically lead to the unsuitability of the member concerned, but requires an assessment by the Board of Directors. The assessment is conducted with regard to the sound and prudent management and safeguarding the Bank's reputation and public trust;

ii) there has been an unjustified absence at two or more consecutive meetings of the Surveillance Body, carried out pursuant to a formal and regular convocation.

[3] With specific reference to the independence requirements, the assessment of the situations relevant for the legislation is performed in relation to the concrete possibility to compromise the independence of mind of the persons concerned, taking into account the specific circumstances and situations.

[4] Reference is made to the requirements set forth by art. 3, 4, 5 of the Ministerial Decree 169/2020, by art. 147-quinquies of the Consolidated Law on Finance and by the Regulation n. 162/2000.

[5] The reference is to the offences in Royal Decree 267/1942 and the offences in the Code of business failure and insolvency (Legislative Decree 14/2019).

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

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

3.6 Grounds for suspension and revocation

The conditions set out below are causes for suspension:

i) a conviction, even if not final, of the member of the Surveillance Body or other sentences would result in suspension from the Board of Directors pursuant to applicable laws;

ii) cases in which after being appointed, members of the Board of Directors are found to have carried out the same role within a company which has received, by non-final measure, the sanctions laid down in Article 9 of the Decree, concerning unlawful acts committed during their term of office;

iii) a non-final sentence, equivalent to the sentence issued pursuant to Article 444 of the Code of Criminal Procedure, even if suspended, for one of the following offences governed by Decree 231/2001; offences concerning corporate failure or insolvency;[6] tax offences;

iv) committal for trial for one of the offences mentioned in the above paragraph;

v) an illness or accident or other justified impediment that continues for over three months, hindering the member of the Surveillance Body from participating therein.

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

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

In the event of suspension of one or more standing members, the Board of Directors shall evaluate the opportunity to order the inclusion in the Surveillance Body of one or more alternate members, taking into account the specific skills of each.

Save for different provisions of the law and regulations, the suspension shall not last beyond 30 days for cases indicated above by i. to iv. and six months for cases indicated above sub v.. After this limit has expired, the Chair of the Board of Directors shall enter the revocation of the suspended member among the items to be addressed in the next Board meeting. Members not revoked shall be fully reinstated in office and the replacing alternate member shall remain as an alternate member.

[6] The reference is to the offences in Royal Decree 267/1942 and the offences in the Code of business crisis and insolvency (Legislative Decree 14/2019).

In the case of illness, accident or justified impediment of a standing member referred to in point v) above, the alternate member takes over after three months, exercising the functions related to the position of member of the SB for no more than one quarter, after which the Chair of the Board of Directors proceeds according to the terms indicated above.

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

i) if it determines that they have been responsible for gross misconduct in performing their duties, upon prior approval of the Management Control Committee, or

ii) pursuant to a justified resolution or upon proposal of the Management Control Committee, adopted unanimously by all members, for any objective reason referring to the improved application of the Model.

3.7 Duties of the Surveillance Body

3.7.1 The Surveillance Body, in pursuit of its ordinary activity shall oversee:

i) the efficiency, effectiveness and adequacy of the Model and the provisions contained therein insofar as preventing the offences covered by Legislative Decree 231/01;

ii) compliance with the provisions of the Model and the provisions referred to therein by its addressees, assessing the consistency of actual behaviour with the Model and any discrepancy, through information flow analyses and reports to be submitted by the heads of the various corporate functions;

iii) updating of the Model as soon as necessary, as a consequence of confirmed and significant breaches of the provisions of the Model, significant changes in the Bank's organisational set-up and procedures, or of the adoption of new legislation in this area, submitting proposals to the competent Corporate Bodies regarding appropriate modifications or integrations;

iv) compliance with the principle and values set forth in the Intesa San Paolo Group's Code of Ethics;

v) the existence and effectiveness of the company's prevention and protections system with regard to occupational health and safety;

vi) the implementation of Personnel training activities (see section 6.3 below);

vii) the adequacy of the procedures and channels for internal reporting of unlawful conducts pursuant to Legislative Decree 231/2001, or any non-compliance with the Model and their suitability in guaranteeing the confidentiality of the person making said reports within the reporting management system;

viii) respect of the ban on "retaliatory or discriminatory actions, whether direct or indirect, against the whistleblower" for reasons directly or indirectly related to the whistleblowing";

ix) the initiation and implementation of the procedure for imposing disciplinary sanctions, by the competent functions, where infringements of the Model are found.

The Surveillance Body shall also monitor, within the scope of its functions and duties, compliance with the provisions relating to prevention of the use of the financial system for the purpose of money laundering and the financing of terrorism laid down in Legislative Decree 231/07.

3.7.2 Pursuant to the aforementioned prerogatives of autonomy and independence of the Surveillance Body, the functioning and observance of the Model are also ensured through constant monitoring, planning, programming and exchange of information flows with corporate bodies and functions.

The Surveillance Body has as its direct contacts and interlocutors, in the performance of its supervisory and control tasks, the heads of the Internal Auditing and Compliance functions (hereinafter: "Surveillance Body Contacts").

The Surveillance Body contacts shall provide, each within his/her purview, adequate support, assistance in the investigations and information to the Body, providing to it all the resources required for such activities, without being required to coordinate among themselves internally, except if the concurrent intervention of all the contacts has been requested.

The relation between the contacts, as well as the personnel they appoint and make available for the specific discovery and investigation requirements, and the Body is fundamental for the optimal performance of the tasks which the Body is specifically assigned and are not of a hierarchical character, notwithstanding the autonomy of the Body's powers of control and its non-involvement in management functions. Indeed, there is no change to the attributions, powers and organisational reporting and functional lines of the Surveillance Board contacts as provided by the Bank's internal organisation and the applicable laws.

The contacts of the Surveillance Body are required to immediately transmit to it all the information acquired by them which are relevant to the Model, in terms of control and monitoring.

When the Body requests the execution of a specific assessment, the involved contacts and the individuals assigned by the latter, are required to maintain the contents of the request they received and the specifically requested investigation activity strictly confidential, except as required by applicable laws. In any case with regard to the outcomes of specifically requested investigation activities, the contacts shall inform the Body of any events or critical issues that render observance of disclosure and reporting obligations necessary pursuant to applicable laws and the Bank's internal regulations.

In order to monitor the specialised regulatory areas, the Surveillance Body shall also enlist the assistance of all functionally competent structures and corporate roles that have been established pursuant to specific sector regulations (Employer, Financial Reporting Officer, Manager of the Prevention and Protection Department, Employee Safety Representative, Competent Doctor, Anti-Money Laundering Department Manager, Head of Suspicious Activity Reporting, Environmental Affairs Officer pursuant to Legislative Decree 152/2006, etc.).

When required due to the need for specialisations which are not available or as appropriate, the Surveillance Body shall enlist the assistance of external consultants to whom it shall delegate technical operations, investigations and the verifications required for conducting its controls.
Whether directly or through various designated corporate structures, the Surveillance Body shall have access to all corporate activities relating to the areas at risk and the relative documentation, whether from the headquarters or the peripheral structures.

3.7.3 In order to allow the Surveillance Body an overview of the planning of the activities for second-level controls (compliance, anti-money laundering, administrative and financial governance) and third-level controls (internal auditing), on an annual basis the Compliance function gathers the respective control activity plans scheduled for the sensitive areas from the relevant structures and integrates these into the "231 Audit Plan".
Based on this document the Surveillance Body assesses the adequacy of the audit plan on the individual sensitive corporate activities and carries out any further action to strengthen the control plans proposed by the individual structures concerned.
The control activity which is set up and organised by internal structures is based on specific protocols designed and regularly updated based on the results of the risk analysis (i.e. the ongoing process of prior identification, classification and assessment of the risks (whether internal or external) and of the internal controls, which is the basis for the 231 Audit Plan and the control interventions.
This plan, prepared annually and submitted for approval to the Surveillance Body, also takes into account any remarks and suggestions made in various respects by the Corporate bodies.
The Control Functions shall periodically report to the Surveillance Body on this activity.

3.7.4 If considered necessary or advantageous, the Surveillance Body may exchange information with the independent auditors.

3.7.5 The members of the Surveillance Body may participate in joint meetings with the Management Control Committee and/or with other Committees on issues of common interest. For issues that fall under the Board of Directors' remit, -the Body may request the Chair of the Board - and in particularly significant cases - the Managing Director and CEO, for specific information on issues which it considers appropriate to examine in order to better conduct its duties of monitoring the operation, efficacy and observance of the Model.

3.7.6 In Chapter 4 below, we describe the information flows towards the Surveillance Body, notwithstanding any additional procedures for the reconciliation and exchange of information between the Surveillance Body and the Board of Directors, the Management Control Committee and other internal control functions of the Bank are further, defined within the Integrated Internal Control System Regulation.

3.8 Procedures and frequency for reporting to the Corporate Bodies

Whenever it is deemed necessary or advisable, or if requested, the Surveillance Body shall report to the Board of Directors and the Management Control Committee on operation of the Model and the fulfilment of the obligations laid down in Legislative Decree 231/01.
The Surveillance Body shall, at least on a half-yearly basis, submit to the above-mentioned Bodies a specific report on the adequacy of and compliance with the Model, which shall refer to:

- the activity carried out;
- the results of the activity carried out;
- the planned corrective and improvement actions and their progress.

4.1 Information flows in the case of particular events and in the event of whistleblowing

The Surveillance Body must be informed, by means of information provided by the Employees, the Heads of the Corporate Functions, the Corporate Bodies, the external parties (meaning suppliers, agents, consultants, independent professionals, self-employed or "para-subordinate" workers, commercial partners etc.) about any events which may give rise to liability for Intesa Sanpaolo S.p.A. pursuant to the Decree.

In particular, any detailed information based on precise and consistent evidence must be reported without delay, concerning:

- the perpetration, or the reasonable conviction of the perpetration, of the offences within the scope of Legislative Decree 231/01;
- breaches of the conduct or procedural rules laid down in this Model and the internal regulations referred to in it;
- initiation of judicial proceedings against recipients of the Model for offences provided for by Legislative Decree 231/01.

Such events can be reported, also anonymously:

- directly to the Surveillance Body by
  - letter addressed to "Intesa Sanpaolo S.p.A. – Organismo di Vigilanza, Via Monte di Pietà 8, 20121 Milan";

  or
  - email to"OrganismoDiVigilanzaDL231@intesasanpaolo.com";
- via the Internal Auditing function, to which the report can be made either directly or through their department/unit head. After duly investigating the matter, the Internal Auditing function informs the Surveillance Body of any reports received and provides a statement of any related facts discovered.

The external parties shall submit their reports directly to the Surveillance Body by one of the above-mentioned methods.

Moreover, pursuant to various legislation that requires the adoption of internal systems to report violations of provisions governing specific sectors (Consolidated Banking Act, Consolidated Law on Finance, anti-money laundering regulations, etc.), these disclosures may be made by personnel[7], who must be named, according to the provisions in the Group Rules on internal systems for reporting violations (Whistleblowing), sending an email to segnalazioni.violazioni@intesasanpaolo.com. This email address is accessed by the Chief Audit Officer (in a capacity as "Head of internal reporting systems) and his/her Delegated Staff Member. If, due to the nature of the whistleblowing, the Chief Audit Officer structure may potentially be involved in a conflict of interest, a "backup" channel is available, as an alternative, managed by the Management Control Committee: segnalazioniviolazioni.comitatoperilcontrollo@intesasanpaolo.com.
Whistleblowing received as above, is initially reviewed then sent to the competent function - identified based on the case in question - in order to start necessary investigations.

The appointed function, as indicated in the "Group Rules on internal systems for reporting violations (Whistleblowing)", shall promptly notify the Surveillance Body (OdV), in the case of sensitive issues pursuant to Legislative Decree 231/01.

The Surveillance Body assesses information received directly and adopts measures under its responsibility and at its discretion, consulting the whistleblower and/or person responsible for the alleged infringement and justifying any refusal to proceed with an internal investigation in writing. The Surveillance Body will consider information, even if reported anonymously, which contains factual elements.
Intesa Sanpaolo S.p.A. shall safeguard those making said reports, irrespective of the channel used, from any type of retaliation, discrimination or penalisation and shall in any event maintain the highest confidentiality on their identity, except where their disclosure is required by the law. Pursuant to Article 6 of the Decree:

- retaliatory or discriminatory acts, whether direct or indirect towards the whistleblower for reasons connected to the report, directly or indirectly, are prohibited. Retaliatory dismissals and organisational measures that have direct or indirect negative effects on working conditions are void, if it cannot be demonstrated that they are not retaliatory in nature and that they are based on reasons extraneous to the report;
- the adoption of discriminatory measures can be reported to the national labour inspectorate;
- the disciplinary system provided for by the Decree, the implementation of which established the penalties indicated further on in Chapter 5, also applies to:

[7] In accordance with the Group Rules on internal systems for reporting violations (Whistleblowing), "staff" means: "employees as well as those collaborators in a business relationship, outside of the organization".

- those who violate the confidentiality requirement on the identity of the whistleblower or the prohibition on retaliatory or discriminatory acts;
- those who report events that are unfounded with gross negligence or intent.

In addition to the reports on the above-mentioned breaches, the following information shall be submitted to the body on a mandatory basis and immediately:

- via the Internal Auditing or Legal function, any information concerning: the measures and/or information issued by judicial police bodies or any other authority, without prejudice for the secrecy obligations laid down in the law, indicating that investigations are in progress, also against unknown persons, for offences falling within the scope of Legislative Decree 231/01, if such investigations concern the Bank or its Employees or Corporate bodies or in any case involve the Bank's liability;
- through the Internal Auditing function, regarding facts, acts, events or omissions indicating the risk of infringement of the rules of the Decree, observed by the corporate control functions as part of their activity and the relative mitigation actions.

Each company structure given a specific role in a phase of a sensitive process must promptly notify the Surveillance Body of its conduct that significantly differs from the conduct described in the process, and the reasons making this deviation necessary or appropriate.
In the case of events which might give rise to serious liability for Intesa Sanpaolo S.p.A., the Internal Auditing function, acting in accordance with Legislative Decree 231/01, shall promptly inform the Chair of the Surveillance Body and shall prepare a specific report describing in detail the event, the risk, the staff involved, the disciplinary measures adopted and the solutions put in place to avoid recurrence of the event.

4.2 Periodic information flows

The Surveillance Body also performs its control tasks by analysing the systematic periodic information flows submitted by the functions performing first-tier control activity (Organisational units), by the Compliance, Internal Auditing, Anti-Money laundering functions and, with regard to specialised regulatory aspects, by the competent internal structures and by the corporate officers established pursuant to specific sector regulations.

Information flows from the Organisational Units

Once a year, the heads of the Organisational Units involved in "sensitive processes" within the meaning of Legislative Decree No 231/01 shall perform a self-assessment review of the activities

carried out to verify the degree of Model implementation, with special regard to compliance with control and conduct principles and with operating rules.

Through this formal self-assessment exercise, they highlight any problem areas in the processes they operate, any departures from the guidelines set out in the Model or in general from the regulatory framework, and the adequacy of such regulations, and shall highlight the actions and initiatives adopted or planned to address such problems.

The Organisational Units' assessments shall be sent once a year to the Compliance function, which shall file these reports, keeping them available for the Surveillance Body to which it shall forward a report setting out the results.

The method for implementing the self-assessment exercise, which falls under the Bank's broader Operational Risk Management process, must be submitted to the Surveillance Body for prior approval.

Information flows from the Compliance function

The reporting flows from the Compliance function to the Surveillance Body consist of:

- annual reports, describing the results of the activity carried out concerning the Model's adequacy and functioning, as well as the changes made to the processes and procedures, (making recourse, for that purpose, to the collaboration of the Organisation, Process Management and Development functions) and the planned corrective and improvement actions (including training actions) and their progress;
- annual 231 Audit Plan, deriving from the integration into a single document of the set of sensitive area control activities planned by the Compliance function and by the Internal Auditing, Anti-money Laundering and Administrative and Financial Governance functions; the aim of this document is to offer the Surveillance Body a complete overview of the second and third-level control actions taken by the structures responsible for the controls within each sensitive area.

Both documents shall be updated on a half-year basis.

Information flows from the Internal Auditing function

The ordinary reporting flow from the Internal Auditing function to the Surveillance Body shall consist of six-monthly and annual reports, informing the Surveillance Body of the checks carried out, and the control actions planned for the subsequent six months, in line with the annual Audit Plan. Within the scope of the reporting flow, summary evidence is provided for notifications that, upon further investigation, displayed matters relevant to Legislative Decree 231/01. Evidence is

also provided of the outcome of checks carried out on the outsourcing of so-called FEI - Critical or Important Functions.

Where it deems it necessary, the Surveillance Body shall request from the Internal Auditing a copy of the detailed report in order to review specific matters it wishes to address more in depth.

Information flows from the Anti-Money laundering function

The periodic reporting flows from the Anti-Money laundering function to the Surveillance Body consist of the six-monthly and annual reports on the control activities performed, the actions taken, the inefficiencies identified and the related corrective actions to be taken, as well as employee training activities. In this context, information is also provided on the oversight of corruption risk.

Information flows from the Risk Management function

The periodic reporting flows of the Risk Management function to the Surveillance Body consist of the annual report of the Chief Risk Officer which summarizes the checks carried out, the results that emerged, the weaknesses identified and the actions to be taken to remove them and in the Dashboard of the critical issues of the Chief Risk Officer presented every six months.

Information flows from the Employer pursuant to Legislative Decree 81/08

The reporting flow from the Employer pursuant to Legislative Decree 81/08 to the Surveillance Body consists of reports with at least annual frequency describing the results of the activity carried out having regard to organisation and to the controls performed on the company's Health and Safety management system.

Information flows from the Principal pursuant to Legislative Decree 81/08

The reporting flow from the Principal pursuant to article 88 and following articles of Legislative Decree 81/08 to the Surveillance Body consists of reports with at least annual frequency informing on the results of the organization and control activities on the company's safety and health management system in temporary or mobile construction sites.

Information flows from the Environmental Affairs Officer

The reports submitted by the Environmental Affairs Officer pursuant to Legislative Decree 152/06 to the Surveillance Body are focused on the annual report on compliance with the provisions of the environmental laws and the monitoring of any legislative amendments and changes, as well as the outcome of the organisation and control activities as applied to the environmental management system.

Information flows from the ESG & Sustainability function

The reporting flow from the ESG & Sustainability function to the Surveillance Body consists of the "Annual report on the adoption and governance of the Code of Ethics" of the Intesa Sanpaolo Group.

Information flows from the Manager responsible for preparing the Company's financial reports pursuant to Article 154-*bis*, Legislative Decree 58/98 (Finance Consolidation Act)

The reporting flows from the Manager responsible for preparing the Company's financial reports to the Surveillance Body consist of the periodic reports envisaged in the "Administrative and Financial Governance Guidelines".

Information flows from the Human Resources function

The reporting flow from the Human Resources function consists of a report submitted at least six-monthly on the disciplinary measures taken against staff during the reporting period with particular attention being given to events directly or indirectly connected to reports of unlawful conduct pursuant to the Legislative Decree or any non-compliance with the Model. Where measures concern facts, acts, events or omissions with serious risks in relation to infringement of the rules of the Decree, specific information may be provided in addition to ordinary reporting.

Information flows from the Organisation function

The reporting flow from the Organisation function consists of a report submitted once a year on the main changes in the organisational structure, their significance pursuant to Legislative Decree 231/01 as well as the degree of alignment of the system of delegated powers.

5.1 General principles

Model effectiveness is ensured – in addition to the adoption of decision-making and control mechanisms such as to eliminate or significantly reduce the risk of commission of the crimes and administrative offences covered by Legislative Decree 231/01 – by the disciplinary instruments established to control compliance with the required conduct.

Any conduct of the employees of Intesa Sanpaolo S.p.A. (including those recruited and/or working abroad) and of the external parties (meaning self-employed or "para-subordinate workers", freelance professionals, consultants, agents, suppliers, commercial partners, etc.) which are not in line with the principles and the rules of conduct laid down in this Model – including the Code of Ethics, the Group's Internal Code of Conduct, the Group's Anti-Corruption Guidelines and the internal procedures and rules, which are an integral part of the Model – shall constitute a breach of contract.

Based on this premise, the Bank shall adopt:

- towards its employees in service through a contract governed by Italian law and through national bargaining agreements for the sector, the system of sanctions laid down in the Bank's Disciplinary Code and in the applicable laws and regulations on contracts;
- towards its employees recruited abroad and in service through a local contract, the system of sanctions established by the laws, regulations and provisions on contracts governing the specific type of employment relationship;
- towards external parties, the system of sanctions laid down in the contractual and legal provisions governing this area.

The initiation of action on the basis of the reports submitted by the competent functions of the Bank or Surveillance Body, the implementation and finalisation of the disciplinary proceeding in respect of the employees shall be carried out, within the limits of its competences by the Human Resources functions.

The penalties against external parties shall be implemented by the function that manages the contract or with which the self-employed worker or the supplier works.

The type and size of each of the sanctions established shall be defined, pursuant to the above-mentioned legislation, taking into account the degree of recklessness, lack of judgement, negligence, fault, or wilfulness of the conduct relating to the action/omission, also considering any repetition of the misconduct, and the work activity carried out by the person concerned and his functional position, together with any other relevant circumstances characterising the fact.

Such disciplinary action shall be pursued regardless of the initiation and/or performance and finalisation of any criminal judicial action, since the principles and the rules of conduct laid down in the Model are adopted by the Bank in full autonomy and independently of any criminal offences which said conduct may determine and which it is for the judicial authority to ascertain.

Therefore, in application of the above-mentioned criteria, the following system of sanctions is established.

The Surveillance Body is responsible for verifying the adequacy of the system of sanctions and constantly monitoring the application of sanctions to employees, and the actions in respect of external parties. The Surveillance Body shall also receive a report at least six-monthly from the Human Resources function on any disciplinary actions taken against employees during the reporting period.

The system of sanctions envisaged for employees (professional areas, middle managers and executives) serving under an employment contract governed by Italian law is detailed below.

5.2 Professional and middle management staff

1) a **verbal warning** shall apply in the event of:

minor breach of the principles and of rules of conduct laid down in this Model or breach of the internal rules and procedures set out and/or referred to, or adoption, within the sensitive areas, of a conduct which is not in line with or not appropriate to the requirements of the Model, such conduct is equivalent to a "*slight breach of the contractual rules, company rules or of the directives or instructions issued by management or by one's superiors*" in the formulation already provided in **point a)** of the current Disciplinary Code;

2) a **written warning** shall apply in the event of:

failure to comply with the principles and of rules of conduct laid down in this Model or breach of the internal rules and procedures set out and/or referred to, or adoption, within the sensitive areas, of a conduct which is not in line with or not appropriate to the requirements of the Model, where such non-compliance is assessed to be neither minor nor serious, such conduct is equivalent to a "*non-serious breach of the contractual rules, company rules or of the directives or instructions issued by management or by one's superiors*" in the formulation already provided in **point b)** of the current Disciplinary Code;

3) **suspension from work without pay for up to 10 days** shall be applied in the event of:

failure to comply with the principles and of rules of conduct laid down in this Model or breach of the internal rules and procedures set out and/or referred to, or adoption, within the sensitive areas, of a conduct which is not in line with or not appropriate to the requirements of the Model, where such non-compliance is assessed to be relatively serious and/or has occurred repeatedly,

such conduct is equivalent to a *"repeated or relatively serious breach of the contractual rules or of the directives and instructions issued by management or by one's superiors*" in the formulation already provided in **point c)** of the current Disciplinary Code;

4) **dismissal for substantiated reasons** shall apply in the event of:
adoption, in performance of the activities belonging to the sensitive areas, of a conduct characterised by serious non-compliance with the requirements and/or the procedures and/or the internal rules laid down in this Model, where it is even simply liable to give rise to one of the offences covered by the Decree,
correlating said behaviour to a " *violation (...) such as to constitute (...) a "significant" non-fulfilment of the relative obligations* " pursuant to the provisions of **point d)** of the current disciplinary code;

5) **dismissal for just cause** shall apply in the event of:
adoption, in performance of the activities belonging to the sensitive areas, of a conduct wilfully in contrast with the requirements and/or the procedures and/or the internal rules laid down in this Model, which, albeit it is simply liable to give rise to one of the offences covered by the Decree, impairs the relationship of mutual trust which characterises employment relationships, or is so serious as to impede continuation of employment, even temporarily,
as such conduct is linked to an "*infringement/fault of such seriousness (either because the act was intentional, or on account of its criminal or monetary consequences, or for its repeated occurrence or its particular nature) that it impairs the trust on which an employment relationship is based and prevents in any case the continuation, even temporarily, of employment*" in accordance with **point e)** of the current Disciplinary Code.

5.3 Executives

Where executives infringe the internal principles, rules and procedures set out in this Model or adopt, in performing the activities belonging to the sensitive areas a conduct not in line with the requirements of the Model, such persons shall incur the measures indicated below, which shall be applied having due regard to the seriousness of the infringement and to whether it is a repeat occurrence. Also in consideration of the particular fiduciary relationship existing between the Bank and executive level employees, in compliance with the applicable provisions of the law and with the National Collective Employment Contract for Executives in credit companies, **dismissal with notice and dismissal for just cause** shall be applicable for the most serious infringements.
As said measures involve termination of the employment relationship, the Company, acting in accordance with the legal principle of applying a graduated scale of sanctions, reserves the right, for less serious infringements, to apply the **written warning** – in cases of mere failure to apply

the principles and rules of conduct set out in this Model or of infringement of the internal rules and procedures set out and/or referred to, or of adoption, within the sensitive areas, of a conduct non complying with or not appropriate to the requirements of the Model – or alternatively, to apply **suspension from work without pay for up to 10 days** – in the event of negligent infringement of duty to a non-negligible degree (and/or repeated) or of negligent conduct infringing the principles and rules of conduct provided for by this Model.

5.4 Employees in service under a foreign contract

For employees in service under a foreign contract the system of sanctions is that envisaged in the local regulations specifically applicable.

5.5 External parties

Any conduct adopted by external parties not belonging to the Bank which, in conflict with this Model, may give rise to the risk of occurrence of one of the offences covered by the Decree, shall, in accordance with the specific terms and conditions of contract included in the letter of appointment or in the agreement, produce early termination of the contractual relationship, without prejudice to any further remedy available to the Bank in the event that it suffers real damage as a consequence of such conduct, e.g. where the Judicial Authority applies the sanctions set out in the Decree.

5.6 Members of the Board of Directors

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

CHAPTER 6 INTERNAL TRAINING AND COMMUNICATION

6.1 Introduction

The administrative liability regime laid out by the law and the Organisational, Management and Control Model adopted by the Bank form an overall system which must be reflected in the operational conduct of the Bank's Staff.

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

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

6.2 Internal communication

On being hired, new staff members receive, together with the required recruitment documents, a copy of the Group's Model, Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines. By signing a declaration, staff members confirm they have received the documents and have read them fully, and undertake to comply with the rules they contain.

The Regulations section of the company's Intranet contains and makes available for consultation the various internal communications, as well as the Model and associated rules (in particular the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines).

The documents published on this site are regularly updated to incorporate any intervening changes in the legislation and in the Model, the periodic updates to which are communicated to all employees by the top management.

Internal communications in support of the Decree and the Model use a variety of tools.

The "Internal News" website, also available on the Intranet and the Web TV, both Live and On Demand, are tools able to provide the Staff with real-time updates on all new matters; the Web

TV, in particular, through video clips that also include interviews with the various department Heads, is a tool able to provide additional information on applicable legislation, “sensitive” activities, training actions, etc..

Moreover, the house organ and the publication of communications material for widespread disclosure (e.g. guidebooks/monographs) are tools designed to host regular features addressing specific matters in depth, which are also prepared with the help of experts, along with input regarding the Decree that aims to encourage the dissemination and consolidation of awareness of corporate administrative liability.

In summary, all the instruments mentioned above, together with the in-house communications and circular notices, ensure that all Staff members receive exhaustive and prompt information at all times.

6.3 Training

The training initiatives aim to make the Decree and the new Model known and, in particular, appropriately support those who are involved in “sensitive” activities.

To ensure it would be effective, the training provided takes into account the many variables present in the reference context; in particular:

- the target (the addressees of the actions and their position and role in the organisation);
- the contents (subjects covered, relevant to the individuals’ roles);
- the training delivery tools (live, digital training);
- the training planning and delivery time (the time needed to prepare and implement the training actions);
- the level of commitment required of the trainees (training time);
- the actions necessary to adequately support the training action (promotion, support by the Department heads).

The activities include:

- e-learning training module addressed to the whole Staff;
- specific training modules designed for Staff members operating in the sectors at greater risk of unlawful conduct (in particular, those working in close contact with the Public Administration, those operating in the Procurement or Finance departments etc.);
- other in-depth training tools used via the training platform.

The platform allows each participant to view the baseline training content on Legislative Decree 231/01, as well as any updates to the legislation, and verify how much they have learned through a final examination.

The specific training modules are implemented, where necessary, after using the digital training contents targeted to the entire staff and whose purpose is to disseminate knowledge of the offences, possible types of offences, and specific safeguards relating to different departments, and to refer to the proper application of the Organisational, Management and Control Model. The teaching method is strongly interactive and makes use of case studies.

The digital training and targeted training contents are updated having regard to the developments in external legislation and in the Model. Whenever substantial changes take place (e.g. extension of the scope of the entity's administrative liability to include new types of offences), training contents are suitably supplemented and delivered.

All staff targeted by the various training actions must participate in the training. Participation is monitored by the competent Human Resources department, assisted by the various department/office Heads, who will in particular be responsible to ensure that their subordinates actually take advantage of the distance learning training initiatives.

The Training function shall collect the attendance data relating to the various training programmes and store such data in a manner readily available to the entities concerned.

The Surveillance Body shall monitor the progress of the training activities also by means of the information forwarded by the Compliance function, and may request periodic checks on the Staff's level of knowledge of the Decree, of the Model and of its operational implications.

CHAPTER 7 PREDICATE OFFENCES - AREAS, ACTIVITIES AND ASSOCIATED RULES OF CONDUCT AND CONTROL

7.1 Identification of the sensitive areas

Article 6, paragraph 2 of Legislative Decree 231/01 provides that the Model shall "identify the activities within which offences may be committed".

The predicate offences covered by the Decree have also been analysed, as illustrated in paragraph 2.4; the business areas of the Bank which are at risk of offences being committed have been identified for each category.

For each area, the various sensitive activities have been identified and the control principles and rules of conduct to be applied by all the persons assigned to those areas have been defined.

The Model is fully implemented in the Company's operations by connecting each area and "sensitive" activity with the corporate structures concerned and with the dynamic management of the processes and of the relevant reference rules.

Under the provisions of the law currently in force, the sensitive areas identified by the Model concern, in general:

- Sensitive area concerning offences against the Public Administration;
- Sensitive area concerning offences of forgery of money (and valuables);
- Sensitive area concerning corporate offences;
- Sensitive area concerning crimes with the purpose of terrorism or subversion of the democratic order, organised crime, transnational crimes and crimes against the person, as well as sports fraud and illegal betting or gaming;
- Sensitive area concerning receipt of stolen goods, money laundering and use of unlawfully obtained money, goods or benefits, as well as self-laundering;Sensitive area concerning crimes against cultural assets ;
- Sensitive area concerning crimes and administrative offences relating to market abuse;
- Sensitive area concerning workplace health and safety offences;
- Sensitive area concerning computer crimes and the unlawful use of non-cash payment instruments;
- Sensitive area concerning crimes against industry and trade and crimes involving breach of copyright and customs' law;
- Sensitive area concerning environmental crimes;
- Sensitive area concerning tax crimes.

7.2 Sensitive area concerning offences against the Public Administration

7.2.1 Offences

Introduction

Articles 24 and 25 of the Decree concern a series of offences laid down in the Criminal Code which have in common the identity of the legal asset they protect, which is the impartiality and sound management of the Public Administration.

The legislator's constant focus on fighting corruption has led to repeated interventions in this area. Over time the punishments have become harsher, new offences have been introduced while others have been amended, including the offence of "*Illegal inducement to give or promise benefits*", which was previously covered by the crime of *"Bribery*" and the offence of "Trafficking of illegal influences". Provision has also been made for the offence of "Private-to-private corruption", as described in paragraph 7.4. Although this is a corporate offence, it is one of the wider measures to combat instances of corruption which can compromise fair competition and the proper functioning of the economic system in general. Further offences were also added for the protection of public finances, both in Italy and in the European Union, including crimes of "Embezzlement" and "Abuse of office".

For the purposes of criminal law a Public Administration Body is defined as being any legal person that pursues and/or implements and manages public interests and which is engaged in legislative, jurisdictional or administrative activity, governed by provisions of public law and which is implemented through instruments issued by the authorities. Purely by way of example, and with reference to the entities typically having relations with the Bank, the following can be identified as being Public Administration Bodies: i) the State, the Regions, the Provinces, the Municipalities; ii) Ministries, Departments, Committees; iii) non-economic public entities (INPS, ENASARCO, INAIL, ISTAT).

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

In short, it should be noted that the distinction between the two profiles is in many cases debatable and blurred, and that it is defined by the above-mentioned provisions according to criteria referring to the objective function performed by such persons.

The title of Public Official is given to those who perform a legislative, judicial or administrative public function. The exercise of an administrative public function is usually associated with those who have decision-making responsibilities or concur to the decision making process of a public body or who

represent the public body in dealings with third parties, and with those exercising authoritative powers or certification powers[8].

Purely by way of example, we may mention the following persons, who have been identified by case law as being Public Officials: court bailiffs, court-appointed technical experts, receivers in bankruptcy cases, tax collectors or executives attached to municipal companies (even if in the form of an S.p.A.), university assistants, postmen, officials at the Italian Automobile Club branch offices, municipal councillors, municipal surveyors, public school teachers, health service officials, notaries and employees of the Italian Social Security Agency, authorised Local Health Service doctors, tobacconists authorised to collect vehicle tax.

The title of Public Service Officer is assigned by exclusion, as it goes to those who perform public interest activities, not consisting of simple or merely material tasks, governed in the same manner as public function, but which do not entail the powers typically assigned to a Public Official.

Purely by way of example, we may mention the following persons, who have been identified by case law as being a Public Service Officer: payment collectors of the National Electricity Company (Enel), gas and electricity meter readers, post office clerks tasked with sorting correspondence, employees of the Italian State Mint, security guards responsible for cash consignments.

It should be noted that under the law, for the purpose of being classified as a Public Official or a Public Service Officer, a person does not necessarily have to be an employee of a Public body: this because in certain particular cases, a public function or public service may also be performed by a private person. With reference to Bank operations, certain specific activities - in particular, those concerning the placement of public debt securities, tax collection, treasury services for a Public Body, investment financing, special or soft loans, can, according to case law, take on public service relevance to the point that the Bank's employees and managers may, in performing those activities, take on the title of public agent, at least as a Public Service Officer. Therefore, employees and officers who in exercising the above-mentioned duties of public importance adopt conduct typical of public agents as described for the offences of bribery, extortion and illegal inducement to give or promise benefits are punished as such and can also trigger the Bank's liability under Legislative Decree 231/01.

The liability of the officers and employees, as well as the entity, can also arise if they adopt conduct with public agents typical of private individuals as described for the above-mentioned offences.

Under Article 322-*bis* of the Criminal Code, the conduct of the private individual – whether as bribe-giver, instigator or as the party induced to give or promise benefits − is a punishable criminal offence not only when involving Public Officials and Persons in Charge of a Public Service within the Italian Public Administration, but also when it involves: i) persons holding corresponding functions or

[8] The concept of "authoritative powers" includes not only coercive powers, but also any discretionary activity carried out in respect of persons who are not on the *same level* as the authority (see Court of Cassation, Joint Sections, ruling 181 of 11 July 1992). The certification powers cover all the activities relating to the issue of documentation having the power of proof under the law, whatever their level.

performing corresponding activities within EU institutions, or within Entities established on the basis of the Treaties establishing the EU, or, lastly, within the other European Union Member States; ii) individuals performing corresponding functions or activities in other foreign states, international public organisations, supranational organisations, international parliamentary assemblies or international courts.

The criminal offences laid down in Articles 24 and 25 of the Decree are summarised below[9].

Embezzlement (Article 314, paragraph 1, and Article 316 of the Criminal Code)

The offence is committed by a public official or a public service officer who appropriates money or movable property of others that has come into his possession or has become available for the purposes of service, or who receives or unduly retains money or other benefits for himself or other parties, perceived by taking advantage of the error of others.

Such conduct involves administrative liability pursuant to Legislative Decree 231/2001 only if the facts harm the financial interests of the EU.

These are disputable offences in situations where the elements of other offences do not occur, such as fraud against the EU.

In banking operations, the offence could be committed by the employee who appropriates, directly or in conjunction with other subjects, also for the benefit of the Bank, sums collected from or intended for customers, when carrying out activities of a public nature, for example in the sector of public financing with EU funds.

Abuse of office (Article 323 of the Criminal Code)

The law punishes any conduct relating to the functions of a public official or public service officer that does not fall within more serious criminal offences, but which in any case is characterized by the intention to procure an unfair financial advantage for oneself or others or to cause others unfair harm.

The conduct must be characterized by:

- the violation of specific rules of conduct expressly provided for by law or by acts having the force of law, from which there is no margin of discretion in decisions;
- the presence of conflict with one's own interest or that of a close relative or other situations which by law require abstention from carrying out the activity.

Such conduct involves administrative liability pursuant to Legislative Decree 231/2001 only if the facts harm the financial interests of the EU.

[9] Articles 24 and 25 of Legislative Decree 231/2001 were modified by Article 5 of Legislative Decree 75/2020 which, starting from 30 July 2020, introduced the new predicate offences of embezzlement, abuse of office, fraud in public supplies, undue receipt of FEA disbursements, fraud and IT fraud against the EU.

In banking operations, these cases could occur when carrying out activities of a public nature, for example in the sector of public financing with EU funds or in a competition with a public official who carries out an undue ruling in favour of the Bank, at the request of Bank staff aware that they are not entitled, even in the absence of promises or donations, which would otherwise constitute crimes of corruption.

Misappropriation of public funds (Article 316-*bis* of the Criminal Code)

This type of offence occurs when, after lawfully receiving loans, subsidies, grants or similar, however called, from the Italian Government, another public body or the European Union intended to achieve one or more purposes, the funds obtained for the purposes for which they were granted are not used. For banks, this type of offence can occur either where the subsidies are directly granted to the Bank for its benefit, or where the Bank takes part, together with the customer, in the funding process in favour of private beneficiaries who are then responsible for the diversion of those funds from their intended public purposes.

Unlawful receipt of public funds (Article 316-*ter* of the Criminal Code)

The offence is committed in the cases in which – by using or submitting false statements or documents or untrue declarations, or by omitting due information – a party obtains grants, aid, financing, subsidised loans or other similar contributions, however called, granted or issued by the State, by other Public Authorities or by the European Union without being entitled to them, as the crime is committed at the time of the funding being obtained. The conduct is punished more severely if it affects the financial interests of the EU and the damage or profit exceeds €100,000. This offence, too, can occur either where the beneficiary of the grants is the Bank itself or where the Bank acts as intermediary in favour of customers responsible for the false declarations or omissions and aids and abets them.

Undue receipt of payments from the European Agricultural Fund (Article 2 of Law 898/1986)

This provision punishes anyone who obtains for himself or for others aid, bonuses, allowances, refunds or payments in general, even if only partially, from the European Agricultural Guarantee Fund or the European Agricultural Fund by showing false data or information. These disbursements are equivalent to the national quotas in addition to those disbursed by the aforementioned Funds, as well as the disbursements made entirely by national finance on the basis of relevant EU legislation.

When the conduct does not only refer to false information, but also to tricks or deceitful deceptions, it considered as a more serious crime of fraud against the State.

Fraud in public supplies (Article 356 of the Criminal Code)

The offence is committed by anyone who fails to fulfil their obligations in the execution of supply contracts with the State, with another public body or with a company providing public services or services for public requirements, by resorting to artifices or deceptions such as to deceive the counterparty over the content of its service, by making all or part of the objects or works necessary for a public establishment or a public service missing.

The penalty is increased if the supply concerns foodstuffs or medicines, or objects or works intended for communications, arms or equipment of the armed forces, or to remedy a common danger or public incident.

Fraud against the State or another public entity (Article 640, paragraph 2, 1 of the Criminal Code)

This type of offence occurs when an unfair profit is obtained by means of artifices or deceits aimed at misleading and causing damage to the State, another Public Body or the European Union.

This offence occurs, for instance, when, in preparing the documents or data required for participating in a tender procedure, the tenderer provides the Public Administration with false information supported by forged documents in order to be awarded the contract.

Aggravated fraud for the purpose of obtaining public funds (Article 640-*bis* of the Criminal Code)

This type of offence occurs when the fraud is carried out for the purpose of unduly obtaining public funds from the State, other Public bodies or the European Union.

The distinguishing features of this offence are the following: compared with the generic fraud offence (Article 640, paragraph 2, 1, of the Criminal Code), this offence is characterised by its specific material object, which is obtaining public funds, howsoever named; compared with the unlawful receipt of public grants (Article 316-*ter* of the Criminal Code), this offence is characterised by the additional use of some artifices or deceits to mislead the granting authority.

Computer fraud (Article 640-*ter* of the Criminal Code)

Computer fraud consists of altering the functioning of an IT or telecommunications system or of tampering with the data, information or software contained therein, obtaining unfair profit. This type of offence is relevant for the purposes of Legislative Decree 231/01 only where it is committed to the detriment of the State, other Public Bodies or the European Union, or if the fact results in the transfer or cash, a monetary value or virtual currency (see section 7.10.1 on this point).

By way of example, such an offence to the detriment of the Public Administration or EU may occur may occur in the event that, once a loan has been obtained, the IT system is tampered with for the purpose of changing the amount of the loan to an amount higher than that lawfully obtained, or

where, the entries of a current account held by a Public Body are changed by unlawfully breaking into a home banking system.

Extortion in office (Article 317 of the Criminal Code)

An active role in the offence of extortion can be played by a Public Official or a Public Service Officer who, abusing of his/her office or powers, forces someone to give or promise to him/her or a third party money or other undue benefits.

The coercion takes the form of violence or threats of undue harm (for example: a refusal to perform an action unless paid to do so), by means that do not leave the freedom of choice to the coerced individual, who is consequently considered the victim of the offence and exempt from punishment.

Therefore liability of the legal entities for extortion arises, provided of interest to or of benefit to the entity, in the case of an offence committed by a senior officer or an employee in one of the following alternative forms:

- extortionate conduct in concert with a Public Official or a Public Service Officer against a third party;
- extortionate conduct in the exercise of certain duties of public importance which, as illustrated in the Introduction, can lead to a bank operator qualifying as a Public Official or a Public Service Officer.

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

This offence punishes the conduct of a Public Service Officer or a Public Official who, abusing of his/her office or powers, induces another person to give or promise to him/her or to a third party money or other undue benefits.

This is an offence different than that of extortion: the pressure and demands of the public agent are not in the form of moral violence typical of extortion, but instead assume forms of mere conditioning of the will of the counterparty, such as describing the potential unfavourable consequences or difficulties, stonewalling, etc.. the conduct of the person submitting to the inducement, paying or promising undue benefits to avoid damage or to achieve unlawful advantage, is also punished. This conduct is punished more severely if it affects the financial interests of the EU and the damage or profit exceeds €100,000.

Therefore corporate liability for illegal inducement can arise, provided of interest to or of benefit to the entity, in the case of an offence committed by a senior officer or an employee in one of the following alternative forms:

- inductive conduct adopted in concert with a Public Official or with a Public Service Officer against a third party;

- inductive conduct adopted in the exercise of certain duties of public importance which, as illustrated in the Introduction, can lead to a bank operator qualifying as a Public Official or public service officer;
- acceptance of inductive conduct from a public official or public service officer.

Bribery

The element common to all cases of bribery against the interests of the public administration consists in an agreement between a public official or a public service officer and a private individual.

The corrupt agreement presupposes that the counterparties act on an equal footing, regardless of which of the two parties initiated the bribery, unlike the situation in cases of extortion in office and illegal inducement to give or promise benefits, which instead requires that the person holding the public office, abusing of such office, exploits his/her superior position vis-à-vis the private party who is in a state of inferiority. Moreover, it can prove difficult in practice to distinguish between instances of bribery and illegal inducement; the distinction is important first and foremost to determine the punishment to be inflicted upon the private individual, which is milder for illegal inducement.

In bribery, two separate offences are distinguished: one is committed by the person receiving the bribe, who holds the public office (passive bribery), the other is committed by the bribe-giver (active bribery), which under the provisions of Article 321 of the Criminal Code is punishable by the same penalties envisaged for the person receiving the bribe. The Bank may be liable for this type of offence committed by its managers or employees, also in its interest or for its benefit in the case of both active and passive bribery. Indeed, as stated in the Introduction, where a bank employee performs activities that can be qualified as public services, such employee may take on the title of public agent.

The following types of bribery are covered by Article 25 of the Decree.

Bribery relating to the exercise of duties (Article 318 of the Criminal Code)

This type of offence occurs when a Public Official or a Public Service Officer receives, for his/her own benefit or for the benefit of others, money or other benefits, or accepts a promise thereof, for performing his/her own duties or exercising his/her own powers. The activity of the public agent can concern either a required act (for example: fast-tracking a procedure which comes under his responsibility), but the offence also exists if the illegal benefit is:

- paid or promised regardless of the identification of a “purchase or sale” in a well-defined act, in that the mere fact that it arises in relation to the general exercise of duties is sufficient;
- paid after an official duty is performed, even if it was not previously promised.

[10]Consequently there are extensive and widely diverse scenarios of subservience to the duty and of donations giving a generic appearance of preferential treatment.

Bribery relating to an act contrary to official duties (Article 319 of the Criminal Code)

This offence, also known as "direct corruption", consists of an agreement relating to the promise or giving of undue payment in relation to an act, to be performed or already performed, that is contrary to the official duties of a public agent (for example, a cash payment for ensuring the award of a contract in a competitive tendering procedure).

Bribery in judicial proceedings (Article 319-*ter*, paragraph 1 of the Criminal Code)

In this type of offence, the conduct of the bribed person and of the bribe-giver is characterised by the specific aim of favouring or damaging one of the parties to criminal, civil or administrative proceedings.

Incitement to bribery (Article 322 of the Criminal Code)

This offence is committed by a private party whose offer or promise or money or of other benefits for the exercise of public office (Article 318 of the Criminal Code) or of an act contrary to official duties (Article 319 of the Criminal Code) is rejected. The same offence applies to a Public Official or a Public Service Officer who solicits such offer or promise without obtaining it.

Trafficking of illegal influences (Article 346-*bis* of the Criminal Code)[11]

A person is guilty of this offence if, by exploiting or asserting existing or alleged relations with a public official or public service officer – or with anyone performing corresponding functions within the European Union, third countries, international organisations or courts – makes an undue promise or gift of cash or other benefits for themselves or for others, as the reward for their illegal mediation, or to remunerate them for the exercise of their duties. Anyone who makes an agreement with the intermediary in relation to this illegal influence will be punished in the same way.

The punishment is harsher in those cases in which the "vendor" of influential relations, whether real or only claimed, is a public official or person in public service, or in cases in which there is an influence on the exercise of judicial activities, or where the objective is to remunerate a public official

[10]Article 318 of the Criminal Code prior to the "anti-corruption law" only contemplated the instance of "improper bribery", i.e. undue payment for performing a specific act, due or in any event compliant with official duties of the public agent. Paragraph 2 envisaged the conduct of "improper bribery after the fact", i.e. undue payment not previously agreed but paid after performance of a specific official act, in which case the person receiving the bribe was punished but not the bribe-giver. Following the repeal of that paragraph, the aforementioned conduct qualifies as under paragraph 1, and consequently both are now punished under such circumstances (see Article 321 of the Criminal Code). Lastly, the title of public employee of the Public Service Officer, which was required in order for the offence in question to apply, is no longer relevant.

[11] This offence was introduced into the Criminal Code by law 190/2012 and was then amended by law 3/2019, which added it to the predicate offences covered by Article 25 of Legislative Decree 231/2001 with effect from 31.1.2019.

or a public service officer to perform an act that conflicts with their official duties, or to omit or delay an official act.

The illegal influence does not have to be actually exercised, for the offence to exist; where this does occur, and where the requirements for the corruption offences governed by Articles 318, 319 and 319-*ter* are met, the parties to the illegal agreement will be punished not by Article 346-*bis*, but on the grounds of conspiracy to commit such offences. This is an offence intended to prevent and punish even the risk of any corruptive agreements taking place.

The law also punishes intermediation through the exercise of public functions – in other words to carry out acts that do not conflict with public duties – which may be a prelude to the corruptive agreements punishable under Article 318 of the Criminal Code. However, lobbying to represent personal interests or to present defence arguments to the authorities through trade associations or qualified professionals, is considered legitimate provided that it is done transparently and correctly, and not in order to obtain undue favours.

7.2.2 Sensitive company activities

The sensitive activities identified in the Model which involve the highest risks of unlawful conduct in relations with the Public Administration are the following:

- Signing contracts with the Public Administration;
- Managing contractual relations with the Public Administration;
- Management of activities relating to a request for authorisation or fulfilment of requirements towards the Public Administration;
- Management and use of the Group's IT systems and Information assets;
- Management of public subsidy schemes;
- Management of funded training;
- Management of litigation and out-of court settlements;
- Management of relations with the Supervisory Authorities;
- Management of the procedures for the procurement of goods and services and for the appointment of professional consultants;
- Management of gifts, entertainment expenses, donations to charities and sponsorships;
- Management of the staff selection and recruitment process;
- Management of real-estate assets and cultural assets assets;
- Management of relations with regulatory bodies.

With reference to the sensitive activity concerning Management and use of the Group's computer systems and Information Assets, see protocol 7.10.2.1; we reproduce hereunder the protocols laying down the control principles and rules of conduct applicable to the other above-mentioned sensitive

activities and which are supplemented by the detailed corporate regulations governing such activities.

Such protocols also apply to the monitoring of any activities performed by Group companies or outsourcers on the basis of special service agreements.

7.2.2.1. Signing contracts with the Public Administration

Introduction

This protocol applies to all the Bank departments involved in the signing of any type of contracts with Public Administration bodies, concerning transactions such as, but not limited to:

- treasury and management, collection and payment services contracts, banking contracts;
- agreements for the provision of investment services (trading, execution of orders, reception and transmission of orders, placement of financial instruments, investment advice);
- contracts/agreements for the disbursement/management of soft financing transactions and/or credit facilities;
- direct financing to public bodies;
- conclusion of lease contracts with public bodies which act as lessors;
- conclusion of agreements with public bodies concerning the offer of banking, investment and insurance products and services to public employees;
- conclusion of agreements with SACE and SIMEST;
- conclusion of corporate contractual relationships and shareholders' agreements with public bodies, for the purpose of establishing and managing equity investments;
- support from consultants prior to the signing of contractual relationships with the Public Administration;
- placement contracts with and without the guarantee/ underwriting of financial instruments issued or held by the Public Administration;
- financial, strategic and business advisory and consultancy services;
- trading in OTC derivatives also carried out in the name and on behalf of other Group companies.

Pursuant to Legislative Decree 231/01, the contract signing process could present opportunities for the offences of "*Corruption against the Public Administration*", in its various forms, of "*Illegal inducement to give or promise benefits", "Trafficking of illegal influences"*[12]*, "Fraud against the State or other public entity" and "Fraud in public supplies*".

The definitions given in this protocol are aimed at ensuring the Bank's compliance with applicable regulations and principles of transparency, correctness, objectivity and traceability in carrying out the activities concerned.

[12] As already stated, under Article 322-*bis* of the Criminal Code, the conduct of the bribe-giver, instigator or person accepting illegal inducement is a punishable criminal offence not only when it involves Public Officials and Public Service Providers within the Italian Public Administration, but also when it involves: i) persons holding corresponding functions or performing corresponding activities within EU institutions, or within Entities established on the basis of the Treaties establishing the EU, or, lastly, within the other European Union Member States; ii) individuals performing corresponding functions or activities in other foreign states, international or supranational public organisations, international parliamentary assemblies or international courts.

Process description

The process for the "*Signing of contracts with the Public Administration*" comprises the following steps:

- commercial development activity and identification of business opportunities;
- management of pre-contractual relations with the Public Administration also in view of the conclusion of ad hoc Agreements between the Public Administration and the Bank;
- participation (where required) in public tendering procedures for the award of the services including:
  - preparing and approving the documentation and forms necessary for participating in the tender procedures;
  - submitting the application for participation in the tender procedure to the Public Body of reference;
  - preparing and approving the documentation and forms necessary for submission of the commercial offer to the Entities;
  - submission of the technical and economic offers to the Public Body of reference;
- conclusion of the contract with the Entity (preparing all the information necessary for the subsequent management of the contract).

The operating procedures for management of the process are governed by the internal rules, which are developed and updated by the competent Structures, and which form an integral and substantive part of this protocol.

Control principles

The control system for monitoring the process described above must be based on the following elements:

- Expressly defined authorisation levels. Specifically:
  - persons exercising authorisation and/or negotiating powers with the Public Administration:
    - are identified and authorised according to their specific role in the organisational code or assigned by the Head of the reference Structure by means of internal delegation, to be kept on file by the same Structure;
    - only operate within the scope/portfolio of customers assigned to them by the Head of the reference Structure;
- acts which involve a contractual commitment on the part of the Bank must be signed solely by duly appointed persons;
  - the power and delegation system establishes management autonomy levels according to type of expenditure and size of the commitment, including towards the Public Administration; internal regulations illustrate the aforementioned authorisation mechanisms, providing an indication of the corporate officers holding the necessary powers.

- Segregation of duties between the persons involved in the process of defining the contractual agreement with the Public Bodies. Specifically:
  - the commercial development activities shall be carried out by different structures from those which manage operationally the delivery of the products/services covered by the contract;
  - definition of the agreement is exclusively entrusted to the Head of the Corporate structure which is competent by reason of the subject of the contract or to duly empowered persons; formal conclusion of the contract shall take place in accordance with the current power and delegation system;
  - the persons tasked with preparing the documentation for submission of the technical and economic offer, or for participation in public calls for tenders, shall be different from those who sign such offers or tenders.

- Control activities:
  - the documentation relating to conclusion of the contractual relationships is submitted for review to the Head of the Corporate structure which is competent by reason of the subject of the contract or to duly empowered persons who, for the purpose of defining new types of contracts, shall avail themselves of the advice of the competent Structure with regard to legal aspects;
  - all the documentation prepared by the Bank for participation in public calls for tenders must be checked, for material and formal truthfulness and congruence, by the Head of the Corporate structure competent by reason of the subject of the contract or by duly empowered persons.

- Process traceability including both the electronic and the paper trail:
  - each key phase of the agreements with the Public Administration must be recorded in writing;
  - any agreement/convention/contract with Public Bodies shall be formalised in a document, which shall be duly signed by persons holding the required powers under the current power and delegation system;
  - in order to allow reconstruction of the responsibilities and of reasons for the choices made, each Structure shall be responsible for filing and storing the documentation falling under its competence, also regrading individual transactions, in telematic or electronic format, as well as the final agreements/covenants/contracts as part of the activities relating to the process of entering into contracts with the Public Administration.

- Bonus or incentive systems: bonus and incentive systems must be able to guarantee compliance with legal provisions, the principles of this protocol and the provisions of the Code of Ethics, also envisaging suitable corrective mechanisms for any conduct deviating from the norm.

Rules of Conduct

The Bank's structures howsoever involved in the activities relating to the conclusion of contractual relationships with the Public Administration, shall comply with the procedures set out in this protocol,

the applicable provisions of the law, the internal rules and any provisions of the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines. Specifically:

- all persons that, during the phase of commercial development and identification of new business opportunities, enter into relations with the Public Administration on behalf of the Bank, must be identified and authorised in accordance with the specific role assigned to them in the organisational code or by the Head of the reference Structure by means of an internal written authorisation kept on record by the Structure in question;
- the persons involved in the process that are responsible for signing acts or documents which are relevant outside the Bank, such as contracts for the sale of services, must be expressly appointed;
- staff members cannot accept any request for undue benefits or attempts at extortion in office by an official of the Public Administration they might receive or simply become aware of, and must immediately report any such cases to their direct superior, who in turn forwards the report received to the Internal Auditing function and Corporate Anti-Corruption Officer for assessment and the completion of any formalities to the Surveillance Body in accordance with the provisions under Chapter 4.1;
- if third parties are to be involved in the process for the conclusion of the contractual relationships with the Public Administration, the contracts entered into with such persons shall contain a specific declaration that they know the provisions of Legislative Decree 231/2001 and the laws against corruption and undertake to comply with them;
- the corporate procedures shall define the criteria and the cases in which the participation of third parties must be first submitted to an independent function for assessment;
- the payment of fees or compensation to external collaborators or consultants involved is subject to permission given in advance by the organisational unit responsible for assessing service quality and the resulting fairness of the fee demanded; in any case, no remuneration shall be payable to employees or external consultants where not fully justifiable by the type of work performed or to be performed.

In any event, it is forbidden to initiate, cooperate/give rise to conduct that could be considered an offence in terms of Legislative Decree 231/2001, and, more specifically by mere way of example, to:

- produce incomplete documents and/or communicate false or altered data and/or omit relevant information on the characteristics of individual transactions;
- adopt deceitful conduct which might lead Public Bodies into error in their choice of procuring services from the Bank or in respect to the characteristics of bank and financial products/services;
- ask or induce members of the Public Administration to grant preferential treatment or omit due information in order to improperly influence the decision to conclude agreements/covenants/contracts with the Bank;
- promise or pay/offer undue sums of money, gifts or free benefits (apart from courtesy gifts of low value) or grant advantages or other benefits of any kind – directly or indirectly, on one's own behalf or for others − to representatives of the Public Administration in order to further or favour the Bank's interests. Examples of such improper advantages include, without limitation, the promise to hire family members and relatives, sponsorship or charity initiatives in favour of related

persons, disbursement of credit under terms not compliant with the principles of sound and prudent management envisaged in company regulations, incentives granted in violation of applicable and company regulations, and more generally, all banking or financial transactions which generate a loss for the Bank and a profit for the aforementioned persons (e.g. unjustified cancellation of a debt position and/or application of discounts or conditions not in line with market parameters);

- promise to pay/offer undue sums of money, gifts or services in kind, benefits of any nature, as described in the previous paragraph, in favour of senior officers or their staff of companies/entities participating in public tenders with a view to persuading them not to participate or to learn of their bids and formulate them in such a way as to ensure they are awarded the contract, or threatening them with unfair damage for the same reasons;
- award appointments to external consultants without following substantiated and objective criteria addressing professionalism and expertise, competitiveness, price, integrity and the ability to provide effective assistance. In particular, the rules for the selection of consultants shall refer to the criteria of clarity and availability of documentary evidence laid down in the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines; this is in order to prevent the risk of bribery offences, in their various forms, and of "*Illegal inducement to give or promise benefits*" and the "*Trafficking of illegal influences*" which could result from the selection of individuals who are "close" to persons linked to the Public Administration and thus the possibility of facilitating the establishment/development of relationships aimed at award of the contract.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.2.2.2. Managing contracts with the Public Administration

Introduction

This protocol applies to all the Bank Structures involved in the management of contractual relationships with Public Administration bodies, concerning transactions such as, but not limited to:

- management of agreements with Public Bodies concerning the offer of banking, investment and insurance products and services to public employees;
- management of treasury and management, collection and payment services contracts, banking contracts;
- management of agreements for the provision of investment services (trading, execution of orders, reception and transmission of orders, placement of financial instruments, investment advice);
- management of taxes acting in the role of withholding agent and authorised collector, and transfer of the tax to the treasury;
- management of the financial transactions with the Bank of Italy and/or the Treasury;
- management of placement contracts with and without the guarantee/ underwriting of financial instruments issued or held by the Public Administration;
- management of financial, strategic and business advisory and consultancy relationships;
- management of trading in OTC derivatives also carried out in the name and on behalf of other Group companies;
- management of the agreements and relations with SACE and SIMEST;
- administrative management of the bonds issued by local authorities and by the State;
- payment of pensions under agreements;
- management of agreements concerning the establishment and management of equity investment relationships with Public Bodies;
- management of the applications and subsequent receipt of contributions/facilities supporting subsidised financing.

Pursuant to Legislative Decree 231/2001, the related processes could present opportunities to commit the crimes of "*Corruption against the Public Administration*" in its various forms, "*Illegal inducement to give or promise benefits", "Trafficking of illegal influences"*[13]*, "Extortion", "Fraud against the State or other public entity", "Misappropriation of public funds", "Aggravated fraud for the purpose of obtaining public funds", "Unlawful receipt of public funds", Embezzlement", "Abuse of*

[13] As already stated, under Article 322-*bis* of the Criminal Code, the conduct of the bribe-giver, instigator or person accepting illegal inducement is a punishable criminal offence not only when it involves Public Officials and Public Service Providers within the Italian Public Administration, but also when it involves: i) persons holding corresponding functions or performing corresponding activities within EU institutions, or within Entities established on the basis of the Treaties establishing the EU, or, lastly, within the other European Union Member States; ii) individuals performing corresponding functions or activities in other foreign states, international or supranational public organisations, international parliamentary assemblies or international courts.

office", "Unlawful receipt of payments from the European Agricultural Fund" and "Fraud in public supplies".

The definitions given in this protocol are aimed at ensuring the Bank's compliance with applicable regulations and principles of transparency, correctness, objectivity and traceability in carrying out the activities concerned.

Process description

The process of managing agreements with the Public Administration comprises the following steps:

- management rates and conditions (authorising the conditions of offer, acquiring and updating data during the procedure);
- maintaining commercial relations with the counterparty.

Management of miscellaneous collections and payments on behalf of Entities to which the Bank provides treasury services is broken down as follows:

- administrative and accounting management of treasury services;
- cash flow reporting to the customer Entities.

The banking contract management process comprises the following phases:

- management of the contract and related formalities
- maintaining contractual relationships with the counterparty.

The process of managing agreements for the provision of investment services (trading, execution of orders, receipt and transmission of orders and placement of financial instruments, investment advice) with public bodies comprises the following phases:

- advice (if any);
- receipt of orders;
- execution of the order;
- confirmation of execution given to the customer;
- liquidation;
- offsetting;
- settlement.

The process of managing taxes acting in the capacity of withholding agent is broken down as follows:

- calculating the tax payable and debiting the amount to the customer (or crediting the amount net of the tax);
- clearance of accounts;

- preparing the form for transferring the tax to the Tax Authority;
- transferring to the Tax Authority.

The process of collecting and transferring the tax on behalf of customers is broken down as follows:

- collection of delegations by the Branches/Tellers or remote channels (internet) and issue of the receipt to customers;
- data processing to obtain the total amounts to be transferred;
- executing the payments (transferring the taxes to the Tax Authority);
- clearance of accounts;
- forwarding reports of payment flows to the Ministry for the Economy and Finance and to the Concessionaires of the collected taxes.

The financial transactions with the Bank of Italy and/or the Treasury Department include the following activities:

- monetary policy transactions through the “repurchase agreement” instrument;
- obtaining intra-day liquidity;
- underwriting of Italian Government Securities;
- currency deposit and trading transactions;
- opening of deposit facilities;
- transactions on behalf of the Treasury (e.g. repurchases, disposals, etc.).

The process to manage placement contracts with and without the guarantee/ underwriting of financial instruments issued or held by the Public Administration comprises the following phases:

- feasibility assessment of the transaction (due diligence);
- approval of the transaction by internal committees where required by the relative regulations;
- marketing activities aimed at contacting potential investors;
- syndication activities (formation of a placement consortium with or without guarantee), structuring of the transaction with the issuer (spread, amount offered, subscription date, maturity date, etc.), registration of the security, etc.;
- stipulation of contracts with counterparties (issuers and consortium members);
- placement with investors (distribution).

The process of managing financial, strategic and business advisory and consultancy relationships with public bodies comprises the following phases:

- preparation and sharing of the work plan with the Public Body (kick off);
- appointment of any external consultants (lawyers, auditors, etc.);
- definition of the deliverables by various consultants;
- analysis and feasibility study of the transaction (definition of the assessment methodology, preparation of the assessment model, due diligence, etc.);
- structuring of the transaction;

- negotiation between the counterparties;
- signing of the contract between the counterparties;
- execution of the contract (signing) of merger, acquisition, divestment and restructuring operations;
- settlement of the transaction (closing).

The process to manage OTC derivative trading, also in the name and on behalf of other Group entities comprises the following phases:

- consultancy and definition of the elements of the contract with the customer or with the Parent Company/other Group company or with the operator of the Parent Company/other Group company;
- receipt of the order;
- execution of the order;
- confirmation of execution given to the customer;
- liquidation;
- offsetting;
- settlement.

Management of the agreements and relations with SACE concerns definition and management of the requirements set out in the Framework Agreement signed with SACE relating to insurance contracts.

Management of the agreements and relations with SIMEST concerns management of the collaboration agreement between the Bank and SIMEST, which relates to a number of legislative instruments including, purely by way of example and without limitation:

- export facilities (Legislative Decree 143/98);
- equity and other investments in foreign companies (Law 100/90);
- financing of commercial participation programmes (Law 394/81);
- participation in international calls for tenders (Law 304/90);
- feasibility studies and technical assistance (Legislative Decree 143/98).

The administrative management of the bonds issued by the Local Authorities includes is broken down as follows:

- recalculation of the rates on the securities included in the managed securities issues;
- payment of coupons and capital repayments at maturity or in advance;
- payment reporting upon maturity of the bonds.

The payment process for pensions managed under agreements includes the following steps:

- management of payments ordered by the Entities which entered into the agreements;

- management of payment of the pensions to beneficiaries;
- checks, where provided for in the agreement, that the pensioners are still alive:
- management of temporary benefits.

The management of agreements concerning the establishment and management of equity investment relationships with Public Bodies is broken down as follows:

- preliminary analysis of the requirements for performing of the contract;
- performance of the contract;
- monitoring of contract performance.

The management of the applications and subsequent receipt of contributions/facilities supporting subsidised financing includes the following steps:

- preliminary verification of eligibility based on regulatory requirements;
- preparing the accounting prospectuses/applications for the contributions and submitting it to the Authority;
- receipt of contributions from the Authority where the contributions are payable to the Bank which already advanced them to the final beneficiary;
- payment of the contributions to the beneficiaries where applicable;
- clearance of accounts;
- verification of any non-performance by the Authorities;
- actions against Authorities in arrears.

The operating methods for managing the process are governed as part of internal regulations developed and updated by the competent Structures, which constitute an integral and substantial part of this protocol.

Control principles

The control system for monitoring the processes described above must be based on the following elements:

- Expressly defined authorisation levels. Specifically:
  - the management of relations with the Public employees during performance of the contractual obligations assumed towards the Authorities is entrusted from the organisational point of view to specific Bank structures which are responsible for the provision of the products/services covered by the contract. Contracts for the provision of services to the Public Administration are concluded in accordance with the rules of conduct set out in the Protocol for the “Conclusion of the contractual relationships with the Public Administration”. In particular, all acts whereby the Bank accepts a contractual obligation towards third parties can only be signed by specifically authorised persons;

- within each Structure, persons exercising authorisation and/or negotiating powers in the management of the contractual relations with the Public Administration:
  - are identified and authorised on the basis of the specific role assigned by the organisational code or by the Head of the reference Structure by means of an internal delegation, kept on file by the same Structure;
  - only operate within the scope/portfolio of customers assigned to them by the Head of the reference Structure;
- different user profiles are defined for accessing IT procedures, matching specific authorisation levels based on assigned functions.

- Segregation of duties between the persons involved in the process of managing contractual agreements with Public Bodies. Specifically:
  - the persons tasked with preparing the reporting documents to be submitted to the Public Bodies shall be different from those who sign such documents;
  - the Structures tasked with the operational management of the products/services covered by the contract shall be different from those tasked with commercial development.

- Control activities: the reference internal set of rules identifies the line controls that must be performed by each Structure concerned when performing accounting/administrative activities relating to performance of the processes subject of this protocol. In particular, the checks shall focus on the regularity of the transactions and on the completeness, the correctness and prompt recording of the accounting entries, which must be constantly supported by maker and checker mechanisms.

- Process traceability including both the electronic and the paper trail:
  - the operations to be performed under contractual obligations with the Public Administration shall include the use of supporting IT systems to ensure traceability of the processed data. The structures shall also file the paper documents relating to the performance of contractual requirements;
  - in order to allow reconstruction of responsibilities, each Structure from time to time concerned shall be responsible for filing and storing, also in telematic or electronic format, all the documentation it produced relating to the management of contractual relationships with the Public Administration.

- Bonus or incentive systems: bonus and incentive systems must be able to guarantee compliance with legal provisions, the principles of this protocol and the provisions of the Code of Ethics, also envisaging suitable corrective mechanisms for any conduct deviating from the norm.

Rules of Conduct

The Bank's structures howsoever involved in the management of relationships with Public Administration Bodies arising from contractual obligations towards such Bodies shall comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and any applicable provisions of the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines.

Specifically:

- the persons involved in the process that are responsible for signing acts or documents which are relevant outside the Bank must be expressly appointed;
- staff members cannot accept any request for undue benefits or attempts at extortion in office by an official of the Public Administration they might receive or simply become aware of, and must immediately report any such cases to their direct superior, who in turn forwards the report received to the Internal Auditing function and Corporate Anti-Corruption Officer for assessment and the completion of any formalities to the Surveillance Body in accordance with the provisions under Chapter 4.1;
- if third parties are to be involved in the management/performance of the contractual relationships with the Public Administration, the contracts entered into with such persons shall contain a specific declaration that they know the provisions of Legislative Decree 231/2001, the provisions of the laws against corruption and undertake to comply with them;
- the payment of fees or compensation to external collaborators or consultants involved is subject to permission given in advance by the organisational unit responsible for assessing service quality and the resulting fairness of the fee demanded; in any case, no remuneration shall be payable to employees or external consultants where not fully justifiable by current or future activities;
- when Treasury transactions with Public Bodies are carried out, or taxes, duties and other contributions are collected at the branches, the transactions shall be carried out following the internal procedures in compliance with the contractual terms and conditions.

In any event, it is forbidden to initiate, cooperate/give rise to conduct that could be considered an offence in terms of Legislative Decree 231/2001, and, more specifically by mere way of example, to:

- produce incomplete documents and/or communicate false or altered data and/or omit relevant information on the characteristics of individual transactions;
- adopt deceitful conduct which might lead Public Bodies into error in their choice of procuring services from the Bank or in respect to the characteristics of bank and financial products/services;
- ask or induce members of the Public Administration to grant preferential treatment or omit due information in order to improperly influence the management of the relationship with the Bank;
- promise or pay/offer undue sums of money, gifts or free benefits (apart from courtesy gifts of low value) or grant advantages or other benefits of any kind – directly or indirectly, on one's own behalf or for others − to representatives of the Public Administration in order to further or favour the Bank's interests. Examples of such improper advantages include, without limitation, the promise to hire family members and relatives, sponsorship or charity initiatives in favour of related

persons, disbursement of credit under terms not compliant with the principles of sound and prudent management envisaged in company regulations, incentives granted in violation of applicable and company regulations, and more generally, all banking or financial transactions which generate a loss for the Bank and a profit for the aforementioned persons (e.g. unjustified cancellation of a debt position and/or application of discounts or conditions not in line with market parameters);

- receive money, gifts or any other benefits or accept the promise of such benefits from any person attempting to obtain a treatment in breach of the legislation or of the provisions issued by the Bank or, in any case, an unduly preferential treatment;
- award appointments to external consultants without following substantiated and objective criteria addressing professionalism and expertise, competitiveness, price, integrity and the ability to provide effective assistance. In particular, the rules for the selection of consultants shall refer to the criteria of clarity and availability of documentary evidence laid down in the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines; this is in order to prevent the risk of bribery offences, in their various forms, of "*Illegal inducement to give or promise benefits*" and the "T*rafficking of illegal influences*", which could result from the selection of individuals who are "close" to persons linked to the Public Administration and thus the possibility of facilitating or influencing the management of contractual relations with the Bank.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.2.2.3. Management of activities relating to a request for authorisation or fulfilment of requirements towards the Public Administration.

Introduction

This protocol applies to all the Bank Structures involved in the management of activities relating to applications for authorisations or the fulfilment of requirements with the Public Administration including, by way of example and without limitation:

- management of relations with social security and social assistance entities, and performance, of labour and social security legal requirements in accordance with the established time limits and procedures (INPS – the National Social Security Agency, INAIL – the National Insurance Agency, INPDAP, Provincial Labour Office, Occupational Medicine, Revenue Agency, Local Public Bodies, etc.);
- management of relations with the Chambers of Commerce for the performance of the activities relating to the Companies' Register;
- management of relations with the Local Authorities competent for waste disposal;
- management of relations with State, Regional, Municipal Administrations and Local Authorities (Local Health Authorities, Fire-fighter Service, ARPA – Regional Environmental Protection Agencies etc.) for the performance of requirements relating to health and safety and/or authorisations (for example building procedures), permits, concessions;
- management of relations with the Ministry of the Economy and Finance, with Customs and Monopolies Agencies, with Tax Agencies and with local Public Bodies for the discharge of tax obligations;
- management of relations with the Bank of Italy for discharge of the obligations relating to compliance with capital reserve requirements;
- management of relations with the Prefecture, Public Prosecutor's Office and Chambers of Commerce which are competent to issue certificates and authorisations;
- management of relations with the Ministry for Economic Development and with the Chambers of Commerce for the discharge of obligations relating to the organisation of prize events (Law 449/97 Article 19 – Presidential Decree 430/2001);
- management of bank information.

Pursuant to Legislative Decree 231/2001, these processes could present opportunities for the offences of "*Corruption against the Public Administration*" in its various forms, of "*Illegal inducement to provide or promise benefits", "Trafficking of illegal influences"*[14]*, "Fraud against the State or other public entity", "Aiding and abetting an offender"* and "*Smuggling crimes".*

[14] As already stated, under Article 322-*bis* of the Criminal Code, the conduct of the bribe-giver, instigator or person accepting illegal inducement is a punishable criminal offence not only when it involves Public Officials and Public Service Providers within the Italian Public Administration, but also when it involves: i) persons holding corresponding functions or performing corresponding activities within EU institutions, or within Entities established on the basis of the Treaties

The definitions given in this protocol are aimed at ensuring the Bank's compliance with applicable regulations and principles of transparency, correctness, objectivity and traceability in carrying out the activities concerned.

Process description

The management of relations with the Public Administration at the time of applying for authorisations or performing legal requirements comprises the following steps:

- preparing the documents;
- submitting the required documents and keeping the file on the record;
- handling relations with the Public Bodies;
- providing assistance during visits and inspections by the Public Bodies;
- managing relations with the Public Bodies for collecting the authorisation and performing the requirements.

The operating methods for managing the process are governed as part of internal regulations developed and updated by the competent Structures, which constitute an integral and substantial part of this protocol.

Control principles

The control system for monitoring the processes described above must be based on the following elements:

- Expressly defined authorisation levels. Specifically:
  - within each Structure, persons exercising authorisation and/or negotiating powers in the management of the activities relating to requests for authorisations to the Public Administration:
    - are identified and authorised according to the specific role assigned by the organisational code or by the Head of the reference Structure by means of internal delegation, to be kept on file by the same Structure; where the relations with the Public Bodies are held by third parties, such parties shall be identified by means of a letter of appointment or in the contractual clauses;
    - only operate within the scope/portfolio of customers assigned to them by the Head of the reference Structure;

establishing the EU, or, lastly, within the other European Union Member States; ii) individuals performing corresponding functions or activities in other foreign states, international or supranational public organisations, international parliamentary assemblies or international courts.

- relations with Public employees in the event of visits/inspections, including those performed to verify compliance with the provisions of law applicable to the activities relating to each area, shall be maintained by the Head of the structure and/or the persons specifically appointed by him/her.

- Segregation of duties between the persons involved in the process of managing the activities relating to requests for authorisations or discharge of obligations towards the Public Administration, in order to ensure that a maker and checker mechanism is in place in all phases of the process.

- Control activities: the activities must be carried out so as to ensure that the data and information accompanying the application for authorisation or supplied in performance of requirements or on request (for example bank evaluations or requests from the Finance Police concerning financial transactions) are truthful, complete, congruent and supplied in a timely manner, with specific controls in the presence of the parties concerned, where appropriate. In particular, where the authorisation/requirement includes data processing in order to prepare the documents requested by the Public Body, the correctness of the processed data shall be checked by persons different from those tasked with performing the activity.

- Process traceability including both the electronic and the paper trail:
  - copy of the documentation delivered to the public body for the request for authorization or for the fulfilment of obligations or upon request (for example bank checks and requests on financial transactions by the Finance Police), is kept in the archive of the competent structure;
  - the Head of the Structure, or another designated staff member shall sign by way of acceptance the report prepared by the Public officials at the time of performing the inspections/visits at the Bank and shall keep a copy on file in his office, together with all annexes;
  - in order to allow the reconstruction of responsibilities and the reasons for the choices made, the Structure from time to time concerned shall be responsible for filing and storing, also in telematic or electronic format, all the documentation it produced relating to performance of the requirements relating to applications for authorisations to the Public Administration.

Rules of Conduct

The Bank's structures howsoever involved in the management of relations with the Public Administration relating to applications for authorisations or the performance of requirements, shall comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and any applicable provisions of the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines.

Specifically:

- the persons involved in the process that are responsible for signing acts or documents which are relevant outside the Bank must be expressly appointed;

- staff members cannot accept any request for undue benefits or attempts at extortion in office by an official of the Public Administration they might receive or simply become aware of, and must immediately report any such cases to their direct superior, who in turn forwards the report received to the Internal Auditing function and Corporate Anti-Corruption Officer for assessment and the completion of any formalities to the Surveillance Body in accordance with the provisions under Chapter 4.1;
- if third parties (freelance professionals, firms etc.) are to be involved in performance of the activities relating to authorisation procedures, or to the performance of requirements towards the Public Administration, the contracts entered into with such persons shall contain a specific declaration that they know the provisions of Legislative Decree 231/2001, the provisions of the laws against corruption and undertake to comply with them;
- the payment of fees or compensation to external collaborators or consultants involved is subject to permission given in advance by the organisational unit responsible for assessing service quality and the resulting fairness of the fee demanded; in any case, no remuneration shall be payable to employees or external consultants where not fully justifiable by current or future activities;
- as part of the audits carried out by Public Administration Officials at the Bank's headquarters, except for situations in which the Officials request direct interviews with specifically identified Bank staff, at least two persons participate in the meetings with the Officials, if belonging to the Structure involved; otherwise, where the audit is carried out by Structures other than the one involved (such as, for example: Human Resources, Organization, Legal, Auditing and Compliance) only one person is expected to attend the meetings with the Officials.

In any event, it is forbidden to initiate, cooperate/give rise to conduct that could be considered an offence in terms of Legislative Decree 231/2001, and, more specifically by mere way of example, to:

- delay without good reason or omit the presentation of documents/communication of requested data;
- provide incomplete documentation and/or communicate false or modified data;
- use deceit which could lead Public Entities into error;
- ask or induce members of the Public Administration to grant preferential treatment or omit due information in order to improperly influence the response of the Public Administration;
- promise or pay/offer undue sums of money, gifts or free benefits (apart from courtesy gifts of low value) or grant advantages or other benefits of any kind – directly or indirectly, on one’s own behalf or for others − to representatives of the Public Administration in order to further or favour the Bank’s interests. Examples of such improper advantages include, without limitation, the promise to hire family members and relatives, sponsorship or charity initiatives in favour of related persons, disbursement of credit under terms not compliant with the principles of sound and prudent management envisaged in company regulations, incentives granted in violation of applicable and company regulations, and more generally, all banking or financial transactions which generate a loss for the Bank and a profit for the aforementioned persons (e.g. unjustified

cancellation of a debt position and/or application of discounts or conditions not in line with market parameters);

- award appointments to external consultants without following substantiated and objective criteria addressing professionalism and expertise, competitiveness, price, integrity and the ability to provide effective assistance. In particular, the rules for the selection of consultants shall refer to the criteria of clarity and availability of documentary evidence laid down in the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines; this is in order to prevent the risk of bribery offences, in their various forms, and of "*Illegal inducement to provide or promise benefits*" and "*Trafficking of illegal influences*" which could result from the selection of individuals who are "close" to persons linked to the Public Administration and thus the possibility of facilitating or influencing the management of contractual relations with the Bank.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.2.2.4. Management of public subsidy schemes

Introduction

This protocol applies to all the Bank Structures involved in the management of the process of disbursing public subsidies to undertakings and/or private individuals, based on regional, national or EU funds.

The management of subsidy schemes includes processing of applications, management and disbursement of the subsidies, which may include, by way of example and without limitations:

- subsidised loans and capital grants issued by the Ministries to support research and development and/or investment projects (e.g. the Sustainable Growth Fund);loans secured from the Guarantee Fund for SMEs pursuant to Law 662/96 or from other national bodies (SACE S.p.A., ISMEA S.p.A.) or supranational bodies (e.g. the European Investment Fund - FEI, or the European Investment Bank - EIB); financing with interest subsidies, financing with third parties' funds (e.g.: EIB, CEB, CDP, Regional Financial Aid, etc.), ordinary loans linked to capital grants or grants for interest relief, also figurative, and loans repayable by the State or covered by State guarantee;
- capital grants for investments and/or research and development, drawing on instruments such as Law 488/92, negotiated programming, regional instruments, etc.;
- discounted purchase of tax receivables sold by a private Customer or entitled company (e.g.: building/renovation work tax bonuses).

The process also includes advice to companies only to access European research and innovation (R&I) funding programs.

Pursuant to Legislative Decree 231/2001, the related processes could present opportunities to commit the crimes of "*Corruption against the Public Administration*" in its various forms, "*Extortion*", "*Illegal inducement to give or promise benefits", "Trafficking of illegal influences"*[15]*, "Fraud against the State or other public entity", "Aggravated fraud for the purpose of obtaining public funds", "Misappropriation of public funds", "Unlawful receipt of public funds", "Embezzlement", "Abuse of office" and "Unlawful receipt of payments from the European Agricultural Fund".*

[15] As already stated, under Article 322-*bis* of the Criminal Code, the conduct of the bribe-giver, instigator or person accepting illegal inducement is a punishable criminal offence not only when it involves Public Officials and Public Service Providers within the Italian Public Administration, but also when it involves: i) persons holding corresponding functions or performing corresponding activities within EU institutions, or within Entities established on the basis of the Treaties establishing the EU, or, lastly, within the other European Union Member States; ii) individuals performing corresponding functions or activities in other foreign states, international or supranational public organisations, international parliamentary assemblies or international courts.

The definitions given in this protocol are aimed at ensuring the Bank's compliance with applicable regulations and principles of transparency, correctness, objectivity and traceability in carrying out the activities concerned.

Process description

The management of subsidies and facilities comprises the following steps:

- advice on Research & Innovation regarding European Funding;
- receiving the applications for subsidies and/or financing (with the preparation of classification lists, where required by the individual subsidy/funding measure);
- examining the applications for subsidies and/or financing and obtaining necessary documentation;
- carrying out investigations, where required, related to the processing of applications for subsidies and/or financing;
- obtaining the documents required by the Public Administration and/or competent guarantor Bodies, certifying the requirements to obtain the document to be admitted to receive subsidies/guarantees; obtaining the documents necessary for the disbursements or for formalising the sale of tax receivables;
- performing the checks, where required, associated with disbursement of the facilities;
- signing the contracts, where applicable;
- request for the funds, where applicable, and disbursement of the facilities and/or the financing;
- periodic request for grants for interest relief;
- payment of funds to bodies (third-party funds), following the collection of payment instalments;
- periodic reporting to the Public Body;
- management of extraordinary company events amending the maintenance of funding, taking place after granting of the facilities (such as changes in the applicant’s corporate structure, mergers, spin-offs, bankruptcy proceedings, transfer of the company's seat, etc.);
- management, were applicable, of repayments and of the debt recovery.

The operating methods for managing the process are governed as part of internal regulations developed and updated by the competent Structures, which constitute an integral and substantial part of this protocol.

Control principles

The control system for monitoring the process described above must be based on the following elements:

- Expressly defined authorisation levels. Specifically:
  - persons exercising authorisation and/or negotiating powers in the management of facilities:

  - are identified and authorised according to the specific role assigned by the organisational code or by the Head of the reference Structure by means of internal delegation, to be kept on file by the same Structure;
  - only operate within the scope/portfolio of customers assigned to them by the Head of the reference Structure;
- all approvals of acts involving the acceptance of obligations by the Bank shall be issued by specifically appointed persons; the internal rules illustrate the above-mentioned authorisation mechanisms, indicating the corporate officials who hold the necessary authorisation powers.

- Segregation of duties between the persons involved, in order to ensure that a maker and checker mechanism is in place in all phases of the process. In particular, where granting of the financing is decided by the Bank, the financing application must be assessed by a different person from the one responsible for issuing the financing decision, except for any exceptions expressly set out in the internal rules applicable from time to time. Furthermore, the persons empowered to grant the financing shall have different decision-making powers according to the customer's creditworthiness ranking (probability of default).

- Control activities: the line controls that must be performed by the Structure competent for the financing granted under Ministerial funds for investment and/or research and development projects include:

  - evaluation and approval, by the heads of the offices/operational teams, of the application assessment reports and of the progress reports on the investments, including the final report;
  - use of IT systems dedicated to the operations, which will include, where possible, appropriate automated control systems.

  As to the structures responsible for managing the other facilities, the line control activity includes in particular:

  - verification, by the examiners in the operations offices, of the economic and capital capacity of applicants, of the technical, economic and financial viability of the projects and of the soundness of the financial plans under assessment;
  - use of IT systems dedicated to operations, which shall include automated control systems (data checks, error warnings, etc.);
  - implementation of signing-off procedures for the main project documents;
  - verification, by the proposing body, that the requirements of eligibility, appropriateness of expenditure and soundness of the financial plan are met;
  - technical check, also by third parties, of the fairness of documented expenditure and of no obstacle to disbursement of the facility;
  - existence of final checks/controls on the correctness of the documentation annexed to each application, by the competent team/operations office;

- any periodic checks to be performed under specific control and monitoring obligations set out in the agreement with the Public Body.

Furthermore, each Structure involved in accounting/administrative activities relating to performance of the processes covered by this protocol shall ensure correct performance of the line control, and checks on the regularity of the transactions and on the completeness, the correctness and prompt recording of the accounting entries, which must be constantly supported by maker and checker mechanisms.

- Process traceability including both the electronic and the paper trail: in order to allow reconstruction of responsibilities and the reasons for the choices made, the Structure from time to time concerned shall be responsible for filing and storing, also in telematic or electronic format, all the documentation it produced relating to performance of the requirements during management of the facilities.
- Bonus or incentive systems: bonus and incentive systems must be able to guarantee compliance with legal provisions, the principles of this protocol and the provisions of the Code of Ethics, also envisaging suitable corrective mechanisms for any conduct deviating from the norm.

Rules of Conduct

The Bank's structures howsoever involved in management of the facilities shall comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and any provisions of the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines. Specifically:

- all persons that, in the application phase or during management of the subsidised loans or grants engage in relations with the Public Administration on behalf of the Bank and those who are responsible for signing acts or documents having external relevance (e.g. application files, requests for funds, etc.) must be identified and authorised according to their specific role assigned by the organisational code or must be expressly authorised;
- staff members cannot accept any request for undue benefits or attempts at extortion in office by an official of the Public Administration they might receive or simply become aware of, and must immediately report any such cases to their direct superior, who in turn forwards the report received to the Internal Auditing function and Corporate Anti-Corruption Officer for assessment and the completion of any formalities to the Surveillance Body in accordance with the provisions under Chapter 4.1;
- if third parties are to be involved in preparation of the financing application/management documents or in the subsequent performance of activities linked to the financed projects/programmes, the contracts/letters of appointment entered into with such persons shall contain a specific declaration that they know the provisions of Legislative Decree 231/2001, the

provisions of the laws against corruption, the provisions of the laws against corruption and undertake to comply with them;

- the payment of fees or compensation to external collaborators or consultants involved is subject to permission given in advance by the organisational unit responsible for assessing service quality and the resulting fairness of the fee demanded; in any case, no remuneration shall be payable to employees or external consultants where not fully justifiable by current or future activities;
- for reasons of incompatibility with the public law role played by the Bank, subsidised loans/capital grants and/or grants for interest relief issued to the enterprises benefiting from the facilities cannot be paid in advance or transferred by the beneficiaries to the Bank responsible for examining the application. Therefore it is strictly prohibited to approve loans or advances with irrevocable payment order or to assign facilities payable to the enterprises whose application is processed by the Bank;
- the Heads of the Structures concerned must ensure, in their respective departments, the ongoing updating and awareness-raising of staff on the reference external legislation and ensure that the staff takes part in the training activities provided by the Bank's central Structures;
- all relations with and obligations towards the Public Administration, or its representatives/officials, shall be carried out with the highest transparency, diligence and professionalism, supplying clear, accurate, complete, faithful and truthful information, and always reporting any conflicts of interest following the established procedure.

In any event, it is forbidden to initiate, cooperate/give rise to conduct that could be considered an offence in terms of Legislative Decree 231/2001, and, more specifically by mere way of example, to:

- knowingly accept and/or present incomplete documents and/or communicate false or altered data;
- use deceit which could lead Public Entities into error;
- ask or induce members of the Public Administration to grant preferential treatment or omit due information in order to improperly influence the management of the relationship with the Bank;
- use grants, subsidies, and public financing granted to the customers for other than their intended purpose in order to procure an advantage for the Bank, also by offsetting said facilities against receivables or by not passing them on;
- promise or pay/offer undue sums of money, gifts or free benefits (apart from courtesy gifts of low value) or grant advantages or other benefits of any kind – directly or indirectly, on one's own behalf or for others − to representatives of the Public Administration in order to further or favour the Bank's interests. Examples of such improper advantages include, without limitation, the promise to hire family members and relatives, sponsorship or charity initiatives in favour of related persons, disbursement of credit under terms not compliant with the principles of sound and prudent management envisaged in company regulations, incentives granted in violation of applicable and company regulations, and more generally, all banking or financial transactions which generate a loss for the Bank and a profit for the aforementioned persons (e.g. unjustified cancellation of a debt position and/or application of discounts or conditions not in line with market parameters);

- accept gifts, advantages of any kind or sums of money from enterprises, yield to recommendations and pressures from said enterprises, in order to facilitate processing of the application and/or ensure granting of the requested facility;
- award appointments to external consultants without following substantiated and objective criteria addressing professionalism and expertise, competitiveness, price, integrity and the ability to provide effective assistance. In particular, the rules for the selection of consultants shall refer to the criteria of clarity and availability of documentary evidence laid down in the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines; this is in order to prevent the risk of bribery offences, in their various forms, and of "*Illegal inducement to give or promise benefits*" and the "*trafficking of illegal influences*" which could result from the selection of individuals who are "close" to persons linked to the Public Administration and thus the possibility of facilitating or influencing the management of the relations with the Bank.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.2.2.5. Financed training management

Introduction

This protocol applies to all the Bank structures involved in the management of the funded training.

Through the management of funded training the Bank, where the requirements are met, obtains training financing, subsidies and grants issued by national and foreign public entities including, by way of example and without limitations, the following instruments:

- European Social Fund (financing for the training of employed/unemployed persons – Community, Regional and Provincial grants);
- Fon. Dir. (National inter-professional fund for the ongoing training of services sector executive employees);
- FBA (Fondo Banche e Assicurazioni [Banks and Insurances Fund]);
- Solidarity Fund for income and employment support and for the professional conversion and professional retraining of credit sector employees.

Pursuant to Legislative Decree 231/2001, the related process could present opportunities for commission of the offences of "*Corruption against the Public Administration*" in its various forms, *"Illegal inducement to give or promise benefits", "Trafficking of illegal influences"*[16], *"Fraud against the State or other public entity", "Aggravated fraud for the purpose of obtaining public funds", "Misappropriation of public funds", "Unlawful receipt of public funds", "Embezzlement" and "Abuse of office".*

The definitions given in this protocol are aimed at ensuring the Bank's compliance with applicable regulations and principles of transparency, correctness, objectivity and traceability in carrying out the activities concerned.

Process description

The process can be broken down as follows:

- identification of initiatives eligible for financing;

[16] As already stated, under Article 322-*bis* of the Criminal Code, the conduct of the bribe-giver, instigator or person accepting illegal inducement is a punishable criminal offence not only when it involves Public Officials and Public Service Providers within the Italian Public Administration, but also when it involves: i) persons holding corresponding functions or performing corresponding activities within EU institutions, or within Entities established on the basis of the Treaties establishing the EU, or, lastly, within the other European Union Member States; ii) individuals performing corresponding functions or activities in other foreign states, international or supranational public organisations, international parliamentary assemblies or international courts.

- preparation and submission of the financing/grant application to Public Body, accompanied, where provided for, by the memorandum of understanding signed with the competent local trade unions;
- implementation of the funded projects;
  - management of the operations relating to the funded initiative;
  - management of the resources provided for by the project/initiative (economic and technical, internal and external);
- cost reporting;
  - collection of accounting data, preparation and drafting of the report;
- management of relations with the Financing Bodies during checks and inspections performed by them;
- management of grant received.

The operating methods for managing the process are governed as part of internal regulations developed and updated by the competent Structures, which constitute an integral and substantial part of this protocol.

Control principles

The control system for monitoring the process described above must be based on the following elements:

- Expressly defined authorisation levels. Specifically:
  - persons who, in the "management of funded training", exercise authorisation and/or negotiating powers in relations with the funding Bodies:
    - are identified and authorised according to the specific role assigned by the organisational code or by the Head of the reference Structure by means of internal delegation, to be kept on file by the same Structure;
    - only operate within the scope assigned to them by the Head of the reference Structure;
  - the financing/grant applications shall be signed by the Head of the competent Structure specifically and formally empowered under the current power and delegation system; the internal set of rules illustrates these authorisation mechanisms, indicating the company staff members to whom the necessary powers are assigned;
  - when the services of external consultants are procured, the appointment process shall take place in accordance with the procedure set up in the dedicated section of this Model (protocol on: "Management of the procedures for the procurement of goods and services and for the appointment of professional consultants"). In any case, consultants shall be selected by collecting a suitable number of offers and choosing among them on the basis of objective and codified criteria.

- Segregation of duties between the persons involved, in order to ensure that maker and checker mechanism is in place in all phases of the process. In particular, the competent Structure shall

assign to each office under its organisational responsibility specific operational and control activities ensuring the separation of roles between the individuals handling the funded training application process and those in charge of the checks.

- Control activity by each competent Structure and in particular:
  - verifying that the contents of the training project are in line with the guidelines set out in the funding call;
  - checking the formal correctness of the documents to be submitted to the Funding Entity in order to participate in the funding call;
  - keeping an attendance record during delivery of the training projects and using supporting IT systems for staff management, recording detailed information on attendance and activities carried out;
  - monitoring the expenditure reporting process throughout, by:
    - collecting and checking the attendance registers, fully completed by participants in the training actions;
    - collecting the documents on the costs for the company of the participating employees/teachers, based on the hourly consideration calculated by the competent office also in view of the participants in the initiative;
    - collecting and checking the fees/invoices concerning the costs incurred for the initiative;
    - verifying the prompt and correct recording of the grants received.

- Process traceability including both the electronic and the paper trail: all the phases of the process are documented, in accordance with the provisions of the funding calls. In particular, each Structure involved in the funded training process shall be responsible for filing and storing, the documentation it is competent for, including the documents sent to the Public financing Entity also by telematic or electronic means.

Rules of Conduct

The Bank's Structures which are howsoever involved in management of the funded training shall comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and any provisions of the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines.

Specifically:

- all persons that, during the subsidised financing or grant application and management process engage in relations with the Public Administration on behalf of the Bank, must be expressly authorised;
- the individuals involved in the process who are responsible for signing papers or documents with external significance (such as applications, feasibility studies, project plans etc.) must be specifically appointed;

- staff members cannot accept any request for undue benefits or attempts at extortion in office by an official of the Public Administration they might receive or simply become aware of, and must immediately report any such cases to their direct superior, who in turn forwards the report received to the Internal Auditing function and Corporate Anti-Corruption Officer for assessment and the completion of any formalities to the Surveillance Body in accordance with the provisions under Chapter 4.1;
- if third parties are to be involved in preparation of the financing application/management documents or in the subsequent performance of activities linked to the financed programmes, the contracts entered into with such persons shall contain a specific declaration that they know the provisions of Legislative Decree 231/01, the provisions of the laws against corruption and undertake to comply with them;
- the payment of fees or compensation to external collaborators or consultants involved is subject to permission given in advance by the organisational unit responsible for assessing service quality and the resulting fairness of the fee demanded; in any case, no remuneration shall be payable to employees or external consultants where not fully justifiable by the type of work performed or to be performed.

In any event, it is forbidden to initiate, cooperate/give rise to conduct that could be considered an offence in terms of Legislative Decree 231/2001, and, more specifically by mere way of example, to:

- present incomplete documents and/or communicate false or altered data;
- adopt deceitful conduct which might lead Public Bodies into error in the technical-economic assessment of the documents submitted;
- ask or induce members of the Public Administration to grant preferential treatment or omit due information in order to improperly influence the decision to grant the funding application;
- use public grants, subsidies and financing for other than the purpose they have been granted for;
- promise or pay/offer undue sums of money, gifts or free benefits (apart from courtesy gifts of low value) or grant advantages or other benefits of any kind – directly or indirectly, on one's own behalf or for others − to representatives of the Public Administration in order to further or favour the Bank's interests. Examples of such improper advantages include, without limitation, the promise to hire family members and relatives, sponsorship or charity initiatives in favour of related persons, disbursement of credit under terms not compliant with the principles of sound and prudent management envisaged in company regulations, incentives granted in violation of applicable and company regulations, and more generally, all banking or financial transactions which generate a loss for the Bank and a profit for the aforementioned persons (e.g. unjustified cancellation of a debt position and/or application of discounts or conditions not in line with market parameters);
- award appointments to external consultants without following substantiated and objective criteria addressing professionalism and expertise, competitiveness, price, integrity and the ability to provide effective assistance. In particular, the rules for the selection of consultants shall refer to the criteria of clarity and availability of documentary evidence laid down in the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines; this is in order to prevent the

risk of bribery offences, in their various forms, and offences of “illegal inducement to give or promise benefits” and the “*Trafficking of illegal influences*”, which could result from the selection of individuals who are “close” to persons linked to the Public Administration and thus the possibility of facilitating or speeding up the handling of the application process.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

The rules of conduct set out in this protocol shall also apply, mutatis mutandis, to any other corporate process concerning the application for and management of public grants/incentives granted to the Bank for any other purpose.

7.2.2.6. Management of litigation and out-of court settlements

Introduction

This protocol applies to all the Bank Structures involved in the management of judicial and out-of-court litigation (administrative, civil, criminal, tax, labour and social security litigation) and out-of-court settlements with Public Bodies or private individuals.

Pursuant to Legislative Decree 231/2001, the related contract signing process could present opportunities for commission of the offences of "*Corruption against the Public Administration*" in its various forms[17], of "*Illegal inducement to give or promise benefits", "Trafficking of illegal influences*"[18], "*Fraud to the detriment of the State or other public entity*" as well as the offence of "*Inducing someone not to make declarations to the Judicial Authority or to make false declarations*"[19].

There is also the risk of commission of the offence of "Private-to-private corruption" and "Instigating private-to-private corruption", described in paragraph 7.4.

The definitions given in this protocol are aimed at ensuring the Bank's compliance with applicable regulations and principles of transparency, correctness, objectivity and traceability in carrying out the activities concerned.

Process description

The litigation management process comprises the following phases, which are pursued under the responsibility of the Structures competent for litigation, in coordination with the Structure concerned by the dispute and with any external professionals appointed:

- opening the judicial or out-of court litigation;
  - collecting the information and documents relating to the dispute;
  - analysing, assessing and submitting evidence;

[17] Therein including bribery in judicial proceedings (Article 319-ter, paragraph 1, of the Criminal Code).

[18] As already stated, under Article 322-*bis* of the Criminal Code, the conduct of the bribe-giver, instigator or person accepting illegal inducement is a punishable criminal offence not only when it involves Public Officials and Public Service Providers within the Italian Public Administration, but also when it involves: i) persons holding corresponding functions or performing corresponding activities within EU institutions, or within Entities established on the basis of the Treaties establishing the EU, or, lastly, within the other European Union Member States; ii) individuals performing corresponding functions or activities in other foreign states, international or supranational public organisations, international parliamentary assemblies or international courts.

[19] This offence, punished by Article 377-bis of the Criminal Code, is a predicate offence of the liability of entities pursuant to Article 25-*decies* of the Decree. Moreover, pursuant to Article 10 of Law 146/2006 it can entail the same liability also where the offence is of transnational scope. An offence is considered to be transnational and is punished with a term of imprisonment whose maximum duration shall be of not less than four years, where it involves an organized criminal group and:

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

  - drafting pleas and briefs and any supplementary documents, directly or in collaboration with the external professionals;
- managing the dispute;
- receiving, analysing and assessing the acts relating to the dispute;
- preparing case files;
- participating in the case, where useful or necessary, in the event of court proceedings;
- liaising constantly with the appointed external professionals, if any, who must be entered in the relevant professional register;
- adopting decisions to:
  - determine the allocations to the Provision for Risks and Charges, concerning the disputes in which the Bank is a defendant, and reporting of the event as operational risk;
  - making payments and reaching out-of-court settlements;
- closing the dispute.

The out-of-court settlement management process covers all the activities necessary to prevent or resolve a dispute through agreements or mutual renunciations and concessions, in order to avoid or close judicial proceedings.

The process can be broken down as follows:

- analysing the event which gave rise to the dispute and assessing whether there are grounds for reaching an out-of-court settlement;
- managing negotiations aimed at identifying and formalising the transaction;
- preparing, signing and implementing the out-of-court settlement.

The operating methods for managing the process are governed as part of internal regulations developed and updated by the competent Structures, which constitute an integral and substantial part of this protocol.

Control principles

The control system for monitoring the process described above must be based on the following elements:

- Expressly defined authorisation levels: the setup for managing the disputes and out-of-court settlements, including with the Public Administration, involves centralising the guidance and/or management and monitoring of individual process phases under different Bank structures depending on whether the nature of the disputes are in the areas of administrative, civil, criminal, fiscal, labour or social security law. Moreover, within each operational phase of the process:
  - the power and delegation system includes clear allocation of powers to settle the disputes, as well as levels of autonomy in respect of litigation management, including in disputes with the Public Administration; the internal rules illustrate the above-mentioned authorisation mechanisms, indicating the corporate officials who hold the necessary powers.

- appointment of legal consultants not included in the list prepared and approved by the competent Structure is subject to authorisation by the Head of the Structure or a duly delegated staff member.

- Segregation of duties: by means of a clear and formalised procedure for the allocation of duties and responsibilities in performance of the activities relating to the management of disputes and out-of-court settlements, including with the Public Administration. In particular, the corporate procedures set out specific value thresholds beyond which individual out-of-court settlements transactions must be authorised by functions different from the business functions that handled the relationship.

- Control activities:
  - periodic detection and monitoring of pending disputes;
  - periodic verification of the regularity, completeness and correctness of all the requirements relating to disputes/out-of-court settlements, which shall be supported by maker and checker mechanisms.

- Process traceability including both the electronic and the paper trail:
  - each relevant phase of the process must be recorded in specific written documents;
  - in order to allow reconstruction of responsibilities and the reasons for the choices made, the Structure from time to time concerned shall be responsible for filing and storing, also in telematic or electronic format, all the documentation under its competence concerning performance of procedures and activities in the management of disputes and out-of-court settlements, including with the Public Administration.

Rules of Conduct

The Bank Structures howsoever involved in management of disputes and out-of-court settlements, including with the Public Administration, shall comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and any provisions of the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines.

Specifically:

- the persons involved in the process and who are responsible for signing acts or documents which are relevant outside the Bank must be expressly appointed;
- if third parties are to be involved in the management of litigation and out-of-court settlement, the contracts/letters of appointment entered into with such persons shall contain a specific declaration that they know the provisions of Legislative Decree 231/2001, the provisions of the laws against corruption and undertake to comply with them;
- the payment of fees or compensation to external collaborators or consultants involved is subject to permission given in advance by the organisational unit responsible for assessing service quality and the resulting fairness of the fee demanded; in any case, no remuneration shall be payable

where it is not adequately justified by the type of work to be performed and/or the value of the dispute in relation to applicable professional fees.

- Staff members cannot accept any request for undue benefits or attempts at extortion in office by an official of the Public Administration they might receive or simply become aware of, and must immediately report any such cases to their direct superior, who in turn forwards the report received to the Internal Auditing function and Corporate Anti-Corruption Officer for assessment and the completion of any formalities to the Surveillance Body in accordance with the provisions under paragraph 4.1.

In any case, it is forbidden to engage in, collaborate with or induce conduct which may belong to one of the types of offences covered by Legislative Decree 231/01; more specifically, purely by way of example and without limitation, with the aim of unduly favouring the interests of the Bank, also through external professionals or third parties, it is forbidden to:

- during formal or informal contact or during all phases of the proceedings:
  - make any undue demand or exercise pressure upon Judges or Members of Arbitration Panels (including ancillary staff and court experts);
  - induce anyone to overstep constraints or thresholds in order to protect the Bank's interests;
  - induce − using violence or threats or, alternatively, by offering or promising money or other benefits − to induce persons to be questioned by the judicial authority and whose statements may be used in criminal proceedings to refrain from answering or to lie
  - unduly influence the decisions of the Adjudicating Body or Public Administration positions when the latter is the adverse party in the dispute/arbitration;
- during inspections/controls/investigations, influence the judgement, opinion, report or appraisal of public bodies or bodies appointed by the Adjudicating Body or Court Police authorities;
- ask or induce members of the Public Administration to grant preferential treatment or omit due information in order to improperly influence the management of the relationship with the Bank;
- promise or pay/offer undue sums of money, gifts or free benefits (outside the scope of practices regarding courtesy gifts of little value) and grant advantages or other benefits of any kind – directly or indirectly, on one's own behalf or for others − to representatives of the Public Administration on a personal basis in order to further or favour the Bank's interests, or threaten them with unfair harm, for the same reasons. Examples of such improper advantages include, without limitation, the promise to hire family members and relatives, sponsorship or charity initiatives in favour of related persons, disbursement of credit under terms not compliant with the principles of sound and prudent management envisaged in company regulations, incentives granted in violation of applicable and company regulations, and more generally, all banking or financial transactions which generate a loss for the Bank and a profit for the aforementioned persons (e.g. unjustified cancellation of a debt position and/or application of discounts or conditions not in line with market parameters);
- award appointments to external consultants without following substantiated and objective criteria addressing professionalism and expertise, competitiveness, price, integrity and the ability to

provide effective assistance. In particular, the rules for the selection of consultants shall refer to the criteria of clarity and availability of documentary evidence laid down in the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines; this is in order to prevent the risk of bribery offences, in their various forms, and of "*illegal inducement to give or promise benefits*" and the "*Trafficking of illegal influences*", which could result from the selection of individuals who are "close" to persons linked to the Public Administration and thus the possibility of facilitating or influencing the management of the relations with the Bank.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.2.2.7. Management of relations with the Supervisory Authorities

Introduction

This protocol applies to all the Bank Structures involved in the management of relations with the Supervisory Authorities, and concerns all types of activity implemented in respect of remarks, requirements, communications, requests and inspections.
With the establishment of the SEVIF (European Financial Supervision System) in Regulations 1092, 1093, 1094 and 1095 of 2010) means that the transfer of supervisory functions at European level now takes place through:

- the Single Supervisory Mechanism (SSM), which gives the ECB tasks and powers of direct, exclusive supervision of major credit institutions;
- the Single Resolution Mechanism (SRM).

Pursuant to Legislative Decree 231/2001, the related process could present opportunities for commission of the offences of "*Corruption against the Public Administration*", in its various forms, of *"Illegal inducement to give or promise benefits*", the "*Trafficking of illegal influences*"[20] and "*Hindering exercise of the functions of Public Supervisory Authorities*" (Article 2638 of the Civil Code).

The contents of this protocol are aimed at ensuring that the Bank complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in handling relations with the Supervisory Authorities, including:

- the European Central Bank;
- the Bank of Italy;
- Consob;
- IVASS;
- Data protection authority;
- the Italian Competition Authority (AGCM);
- COVIP;
- OAM;
- tax supervisory authorities (the Revenue Agency).

The rules of conduct set out in this protocol shall also apply, in terms of general conduct guidelines, to relations with foreign Supervisory Authorities.

[20] As already stated, under Article 322-*bis* of the Criminal Code, the conduct of the bribe-giver, instigator or person accepting illegal inducement is a punishable criminal offence not only when it involves Public Officials and Public Service Providers within the Italian Public Administration, but also when it involves: i) persons holding corresponding functions or performing corresponding activities within EU institutions, or within Entities established on the basis of the Treaties establishing the EU, or, lastly, within the other European Union Member States; ii) individuals performing corresponding functions or activities in other foreign states, international or supranational public organisations, international parliamentary assemblies or international courts.

Process description

The activities relating to the management of relations with the supervisory authorities can be broken down as follows:

- preparing/submitting occasional or periodic reports to the Supervisory Authorities;
- submitting requests/applications for approvals and/or authorisations;
- providing replies and performing requirements in response to requests/demands of the Supervisory Authorities;
- handling relations with Officials of the Supervisory Authorities during inspections;
- monitoring remediation actions and the provision of information to the supervisory authorities by providing periodic reports.

The "Group Rules on the management of relations with regulators and supervisory authorities" identify the Bank departments tasked with coordinating the communications between these authorities and with ensuring that these communications are consistent at Group level (Pivot Structure).

The Pivot Structure will involve the "Functional Owners" on aspects or for contributions pertaining to their respective areas, depending on the object or scope of the contract or issue in question.

In accordance with the company's organisational charts, responsibilities are allocated as follows:

- the Collective Bodies and Corporate Affairs office is responsible for managing official correspondence with the supervisory and resolution authorities, and for managing relations and authorisation procedures involving the regulators in connection with the fulfilment of corporate requirements, by providing advice and legal assistance to the departments and corporate bodies;
- M&A and Group Investments are responsible for the authorisation procedures and/or for making the regulatory reports relating to this function;
- Legal Affairs is responsible for managing administration procedure (preliminary or disciplinary proceedings) and for providing legal assistance and advice, also for the formal submission of pleadings and statements of defence, in relation to any legally significant issues, and in connection with consultations started by the regulatory bodies, it will collaborate with the Functional Owners to assess the legal impact of new rules.

The operating methods for managing the process are governed as part of internal regulations developed and updated by the competent Structures, which constitute an integral and substantial part of this protocol.

Control principles

The control system for monitoring the process described above must be based on the following elements:

- Expressly defined authorisation levels. Specifically:
  - except for site inspections, relations with the Supervisory Authorities shall be handled by the Head of the reference Structure or by persons appointed by him by means of an internal delegation, which shall be kept on file by the Structure;
  - all acts which involve a commitment on the part of the Bank must be signed solely by duly appointed persons;
  - replies to findings raised by the authorities must, where required, be approved and/or examined by the relevant Board committees and by the Board of Directors.

- Segregation of duties between the different persons involved in the process of managing relations with the Supervisory Authorities. Specifically:
  - for relations that do not fall within the scope of the Bank's ordinary operations, all correspondence pertaining to complaints or objections sent to the regulatory authorities in relation to the Bank's activities will be prepared by the Pivot Department, with the support of the functional owner;
  - the Pivot Department will inform Internal Audit of the inspection, as well as the heads of the departments involved who will verify the object of the inspection and will then identify the people responsible for handling the relations with the public officials while they are on the Bank's premises. In particularly important cases the Surveillance Body must be promptly informed of the inspection and of any requests or findings of the Authority.

- Control activities:
  - the controls concerning the completeness, correctness and accuracy of the information provided to the Supervisory Authorities by the Structure concerned as to the activities falling under its competence that must be supported by maker and checker mechanisms;
  - legal controls on compliance with the reference legislation applicable to the requested report/communication;
  - automated system controls concerning periodic reports.

- Process traceability including both the electronic and the paper trail:
  - all the Bank's structures which are howsoever involved in preparing and transmitting communications and required documents to the Supervisory authorities, must file and store the relevant documentation produced in the course of their relations with the Authority, including all documents submitted to the Authority by electronic means. This documentation must be made available on demand to Legal, Internal Audit, Corporate Secretariat and the Pivot Department;

- every communication to the Supervisory Authorities concerning important data and/or information on the Bank's operations shall be documented/recorded in electronic format and kept on file by the competent Structure;
- except where the Supervisory Authority is not required to immediately issue an inspection report, the staff member of the Structure concerned who was present at the inspection shall assist the Public Official in preparing the report of the inspection and findings; the Bank's staff member shall reserve the right to submit any objections, and shall sign the inspection report prepared by the Public Official, to confirm having read the report together with all annexes;
- for every inspection made by Officials representing the Supervisory Authorities the Head of the Structure concerned shall send to the competent Company entities a copy of the inspection report issued by the Public Official complete with its annexes. Where no immediate issue of an inspection report by the Supervisory Authority is provided for, the Head of the Structure concerned by the inspection or the person delegated by him shall prepare a summary report of the inspection visit and shall send it to the competent Company entities. Such documentation shall be kept on file by the Head of the Structure concerned by the inspection.

Rules of Conduct

The Bank Structures howsoever involved in the management of relations with the Supervisory Authorities shall comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and any provisions of the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines.

Specifically:

- the persons involved in the process that are responsible for signing acts or documents which are relevant outside the Bank must be expressly appointed;
- staff members cannot accept any request for inappropriate benefits or attempts at extortion in office by a member of the Supervisory Authority they might receive or simply become aware of, and must immediately report any such cases to their direct superior, who in turn forwards the report received to the Internal Auditing function and Corporate Anti-Corruption Officer for assessment the completion of any formalities to the Surveillance Body in accordance with the provisions under Chapter 4.1;
- the periodic reports to the Supervisory authorities must be submitted in a timely manner and any requests/demands from the same Authorities must be promptly acted on;
- as part of the audits carried out by the Officers of the Supervisory Authorities at the Bank's headquarters, except for situations in which the Officer request direct interviews with specifically identified Bank personnel, at least two persons participate in the meetings with the Officers. Where the audit is followed by Structures other than the one involved (such as, for example: Pivot Structure, Human Resources, Organization, Legal and Auditing) the presence of only one person from the Structure concerned, together with another person from one of these Structures, is sufficient.

In any event, it is forbidden to initiate, cooperate/give rise to conduct that could be considered an offence in terms of Legislative Decree 231/2001, and, more specifically by mere way of example, to:

- delay without good reason or omit the presentation of documents/communication of requested data;
- present incomplete documents and data and/or communicate false or altered data;
- adopt deceitful conduct which might lead the Supervisory Authorities into error;
- ask or induce representatives of the Supervisory Authorities to grant preferential treatment or omit due information in order to hinder performance of Supervisory duties;
- promise or pay/offer undue sums of money, gifts or free benefits (apart from courtesy gifts of low value) or grant advantages or other benefits of any kind – directly or indirectly, on one's own behalf or for others − to representatives of the Public Administration in order to further or favour the Bank's interests. Examples of such improper advantages include, without limitation, the promise to hire family members and relatives, sponsorship or charity initiatives in favour of related persons, disbursement of credit under terms not compliant with the principles of sound and prudent management envisaged in company regulations, incentives granted in violation of applicable and company regulations, and more generally, all banking or financial transactions which generate a loss for the Bank and a profit for the aforementioned persons (e.g. unjustified cancellation of a debt position and/or application of discounts or conditions not in line with market parameters).

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.2.2.8. Management of the procedures for the procurement of goods and services and for the appointment of professional consultants

Introduction

This protocol applies to all the Bank Structures involved in the management of the procedures for the procurement of goods and services.

The term goods shall also include intellectual works[21], the term services shall also include all types of intellectual services (e.g. legal, fiscal, technical, labour consultancy, administrative, organisational, various forms of mediation, agency or brokering assignments, etc.), including professional or consultancy appointments.

Under Legislative Decree 231/2001, this process could be means for the committing of offences of "*Corruption against the Public Administration*" in its various forms, or of "*Illegal inducement to give or promise benefits*", or "*Trafficking of Illegal Influences*"[22].
Indeed, non-transparent process management might allow the commission of such offences, for example by creating "slush funds" after paying prices exceeding the actual value of the good/service obtained.
There is also the risk of the offence of "*Private-to-private corruption*" and "*Instigating private-to-private corruption*", described in paragraph 7.4.

The aim is also to prevent the risk of acquiring illegally obtained goods or services, and to prevent involvement in other crimes the counterparty could be exposed to (crimes against industry and trade); offences of copyright infringement; smuggling crimes, crimes of employment of illegal immigrants and illicit intermediation and exploitation of labour,[23] etc.).

[21] Pursuant to Article 2575 of the Civil Code, intellectual works protected by copyright are those belonging to the sciences, literature, music, the figurative arts, architecture, theatre, and film, irrespective of their form of expression. Computer software and data banks which by their choice of arrangement of materials constitute an intellectual work of their author are also ranked pari passu with literary works and enjoy the same protection (Article 1, Law 633 of 22 April 1941).

[22] As already stated, under Article 322-*bis* of the Criminal Code, the conduct of the bribe-giver, instigator or person accepting illegal inducement is a punishable criminal offence not only when it involves Public Officials and Public Service Providers within the Italian Public Administration, but also when it involves: i) persons holding corresponding functions or performing corresponding activities within EU institutions, or within Entities established on the basis of the Treaties establishing the EU, or, lastly, within the other European Union Member States; ii) individuals performing corresponding functions or activities in other foreign states, international or supranational public organisations, international parliamentary assemblies or international courts.

[23] On this point, see paragraphs 7.5 and 7.11.

The definitions given in this protocol are aimed at ensuring the Bank's compliance with applicable regulations and principles of transparency, correctness, objectivity and traceability in carrying out the activities concerned.

Process description

Management of the procedures for the purchase of goods and services includes the following processes:

- preparing and managing the budget;
- procurement management;
- purchasing cycle management;
- supplier management.

The operating procedures for management of the processes are governed by the internal rules, which are developed and updated by the competent Structures, and which form an integral and substantive part of this protocol.

Control principles

The control system for monitoring the processes described above must be based on the following elements:

- Expressly defined authorisation levels:
  - pursuant to the Articles of Association, the Bank's budget is prepared and approved by the Board of Directors;
  - approval of the purchase request, supplier selection, conclusion of the contract and issue of the order shall be exclusively carried out by persons specifically empowered under the existing power and delegation system, which defines levels of operational autonomy by type and amount of expenditure. The internal set of rules illustrates these authorisation mechanisms, and indicates the corporate officials who hold the necessary powers;
  - the choice of the suppliers of goods and services and of freelance professionals is made from lists of suppliers selected on the basis of criteria identified in the internal set of rules, except for occasional needs/supplies. Such suppliers must ensure and, on demand, must be able to prove by submitting adequate documentation, also with reference to their appointed sub-contractors:
    - in relation to the use of trademarks or distinctive signs and the marketing of goods or services - compliance with regulations industrial property rights and copyright and, in any case, the legitimate origin of the goods supplied and the correct completion of customs procedures (including payment of the related fees);

  - in relation to the workers employed, compliance with immigration laws and regulations relating to pay, contributions, welfare, insurance and taxes;
- any subcontracting of supplies of services/activities by the Bank's suppliers to third parties shall be contractually conditional on prior approval by the Bank structure which signed the contract;
- authorisation to pay invoices shall be issued by the Heads of the Structures responsible for the relevant budget and powers of expenditure (Centres of Responsibility) or by persons delegated by them; authorisation to pay may be denied where the Structures find the supply to be substandard/non-compliant, and issue a formal complaint, which shall be appropriately detailed and accompanied by supporting documents;
- the invoices shall be paid by a specific dedicated Corporate structure.

- Segregation of duties between the different persons involved in the procurement procedure management process. Specifically:
  - the activities relating to the different phases of the process must be carried out by different and clearly identifiable persons, and must be supported by a maker and checker mechanism.

- Control activities: the reference internal set of rules identifies the controls that must be performed by each Structure concerned in each phase of the process:
  - verification of expenditure limit and of appropriateness of the expenditure;
  - checks on the regularity, completeness, correctness and prompt recording of the accounting entries;
  - verification of compliance with the criteria identified by the corporate regulations for the choice of suppliers and freelance professionals (the initiation of the relationship must be preceded by an adequate due diligence, as established by the Anti-Corruption Guidelines), including sample checks regarding compliance of the aforementioned guarantees concerning the authenticity and lawful origin of the goods supplied and the legal status of the workers employed;
  - verification of compliance with legal regulations that forbid or subject to certain conditions the appointment of any kind of public employee or former public employee.

  Lastly, as concerns the assignment of professional commissions and consultancies, the performance of which call for direct relationships with the Public Administration (for instance, legal expenses litigation, fees paid to freelance professionals for building permits, consultants' fees for preparing public grant applications, etc.) the Heads of the Structures concerned must:
  - ensure that a list of freelance professionals/consultants, indicating the object of their commission and the consideration payable, is kept updated and available at all times;
  - regularly check the above-mentioned list to identify any abnormal situations.

- Process traceability including both the electronic and the paper trail:
  - use of IT systems supporting the operations, to ensure that the data and information relating to the procurement process are recorded and kept on file;

- each process phase shall be documented, paying particular attention to the phase of selection of the goods and/or service supplier or the freelance professional, also through competitive bidding procedures, providing reasons for the selection and justifying the appropriateness and congruence of the price. The internal rules indicate in which cases goods and/or service suppliers or professionals must be selected by means of a competitive bidding procedure or in any event by requesting several offers;
- in order to allow the reconstruction of responsibilities and the reasons for the choices made, the Structure from time to time concerned shall be responsible for filing and storing, also in telematic or electronic format, all the documentation it produced in performance of the requirements relating to management of the goods and services procurement process.

Rules of Conduct

The Bank Structures howsoever involved in the management of goods and service procurement procedures or in the professional commission award process shall comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and any provisions of the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines.

Specifically:

- the contractual documents governing the award of supply contracts/professional commissions must contain an ad hoc declaration that the party knows the provisions of Legislative Decree 231/2001, the provisions of the laws against corruption and undertakes to comply with them;
- the payment of fees or compensation to external collaborators or consultants involved is subject to permission given in advance by the organisational unit responsible for assessing service quality and the resulting fairness of the fee demanded; in any case, no remuneration shall be payable to employees or external consultants where not fully justifiable by current or future activities;
- the payments shall be made only into a current account held by the supplier/freelance consultant with whom the relationship has been established;
- payments in cash, payments to a country other than the one in which the counterparty is established or to a party other than the latter shall not be allowed.

In any case, it is forbidden to engage in, collaborate with or induce conduct which may be instrumental to commission of one of the types of offences covered by Legislative Decree no. 231/2001; more specifically, purely by way of example and without limitation it is forbidden to:

- award goods/services supply contracts and professional commissions where no expenditure authorisation has been issued, or where the necessary requirements of professionalism, quality and cost-effectiveness of the goods or services supplied are not met;
- attest to the regularity of the goods/services upon receiving them, without having carefully assessed their actual quality and congruence;
- authorise the payment of goods/services without having checked that they match contract terms and specifications;

- authorise the payment of professionals' fees without having carefully checked the amount of such fees against the quality of the service received;
- make payments to Bank suppliers which are not justified by the contractual relationship in force with them;
- threaten suppliers with retaliation if they provide services to or use the services of competitors of the Bank;
- introduce goods that violate the provisions, prohibitions and limitations set out in the Consolidated Law on customs;
- promise or pay/offer undue sums of money, gifts or free benefits (outside the scope of practices regarding courtesy gifts of little value) and grant advantages or other benefits of any kind – directly or indirectly, on one's own behalf or for others − to officers/representatives of the Public Administration on a personal basis in order to further or favour the Bank's interests, or threaten them with unfair harm, for the same reasons. Examples of such improper advantages include, without limitation, the promise to hire family members and relatives, sponsorship or charity initiatives in favour of related persons, disbursement of credit under terms not compliant with the principles of sound and prudent management envisaged in company regulations, incentives granted in violation of applicable and company regulations, and more generally, all banking or financial transactions which generate a loss for the Bank and a profit for the aforementioned persons (e.g. unjustified cancellation of a debt position and/or application of discounts or conditions not in line with market parameters).

The rules on control and conduct illustrated in this protocol also, where compatible, apply to the leasing of sales or commercial premises to commercial partners

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.2.2.9. Management of gifts, entertainment expenses, donations to charities and sponsorships

Introduction

This protocol applies to all the Bank Structures involved in the management of gifts, entertainment expenses, donations to charities and sponsorships.

For the purposes of this protocol, the following definitions shall apply:

- gifts means goods having a low value which are offered at no charge, in the framework of normal business relations, in order to promote the Bank's business;
- entertainment expenses means the expenses incurred by the Bank in pursuing commercial relations, for the purpose of promoting and improving the Bank's image (for example: costs for lunches and refreshments, expenses for welcome and hospitality activities, etc.);
- charitable contributions means money donations which the Bank makes exclusively to non-profit organisations;
- sponsorships means the promotion, enhancement and strengthening of the Bank's image by concluding atypical agreements (free-form agreements, asset agreements, mutual services agreements) with external organisations (e.g.: sports clubs associations, including amateur associations, non-profit organisations, local agencies and local bodies, etc.).

Under Legislative Decree 231/2001, this process could be means for the committing of offences of "*Corruption against the Public Administration*" in its various forms, or "*Illegal inducement to give or promise benefits"*, or "*Trafficking of Illegal Influences*"[24].

There is also the risk of commission of the offence of "*Private-to-private corruption*" and "*Instigating private-to-private corruption*", described in paragraph 7.4.

This is because non-transparent management of the processes relating to gifts, entertainment expenses, donations to charities and sponsorships could enable the commission of such offences, for example by giving/granting advantages to members of the Public Administration and/or senior officers and/or their staff in companies or entities that are counterparties or in relationships with the Bank in order to favour the Bank's interests or by creating funds that can be used to commit such offences.

[24] As already stated, under Article 322-*bis* of the Criminal Code, the conduct of the bribe-giver, instigator or person accepting illegal inducement is a punishable criminal offence not only when it involves Public Officials and Public Service Providers within the Italian Public Administration, but also when it involves: i) persons holding corresponding functions or performing corresponding activities within EU institutions, or within Entities established on the basis of the Treaties establishing the EU, or, lastly, within the other European Union Member States; ii) individuals performing corresponding functions or activities in other foreign states, international or supranational public organisations, international parliamentary assemblies or international courts.

The definitions given in this protocol are aimed at ensuring the Bank's compliance with applicable regulations and principles of transparency, correctness, objectivity and traceability in carrying out the activities concerned.

Process description

The processes relating to management of gifts and entertainment expenses concern goods intended to be freely given for commercial courtesy purposes to third parties, such as, for example, customers, suppliers, Public Administration Bodies, public institutions or other organisations.
Gifts or other types of presents (such as invitations to sports events, shows and entertainment, tickets, etc.) which originate from or are provided to the same individual/entity which do not exceed the value of Euro 150 in one calendar year are considered to be acts of commercial and/or institutional courtesy of a moderate value.
Such goods are purchased in accordance with the operational rules set out in the internal regulations on expenditure in the protocol "*Management of the procedures for the procurement of goods and services and for the appointment of professional consultants*".

The processes relating to the management of expenses for charity donations and sponsorships comprise the following steps:

- receipt of the request, submitted by the Entities, for grants and donations to charities or sponsorships for projects, initiatives, events;
- identification of the companies/organisations to which the donations will be made;
- performance of the Bank's due diligence activity[25];
- review/assessment of the proposed initiative/project;
- authorisation of expenditure and, if applicable, conclusion of the agreement/contract;
- disbursement of the donations by the Bank.

The operating procedures for management of the processes are governed by the internal rules, which are developed and updated by the competent Structures, and which form an integral and substantive part of this protocol.

Control principles

The control system for monitoring the processes described above must be based on the following elements:

[25] Search for relevant information on the requesting Entity including, for instance and without limitation, its name, legal form and date of establishment, registered office and main operating office (if different from the registered office), website address if any, name of the legal representative and any information regarding his reputation, information on the entity and its key strategies, its size (number of employees and/or collaborators, number of partners), on the main projects implemented in the last two years in the sector addressed by the proposed initiative, summary of the key financial data contained in the approved financial statements of the last two years, etc.

- Expressly defined authorisation levels:
  - with regard to the purchases of goods for gifts and entertainment expenses, approval of the purchase request, supplier selection, conclusion of the contract and issue of the order shall be exclusively carried out by persons specifically empowered under the existing power and delegation system, which defines levels of operational autonomy by type and amount of expenditure. The internal set of rules illustrates these authorisation mechanisms, and indicates the corporate officials who hold the necessary powers;
  - all donation disbursements must be approved by persons duly empowered under the current power and delegation system;
  - Gifts or other presents that exceed the value of Euro 150 may be allowed, on an exceptional basis, in consideration of the profile of the donor or the beneficiary and always within the limits of reason, upon authorization of the individual hierarchically in charge who must be at least a manager or have an equivalent position within the corporate structure. The limits set on the amounts on an annual basis for the gifts and other presence do not apply to entertainment expenses relative to lunches, refreshments, events and forms of hospitality with the participation of corporate representatives and Bank personnel, provided they are strictly related to the business relationship and reasonable as compared to the commonly accepted practices of commercial and/or institutional courtesy;
  - different user profiles are defined for accessing IT procedures, matching specific authorisation levels based on assigned functions;

- Segregation of duties: between the different persons involved in the processes. Specifically:
  - the activities relating to the different phases of the processes must be carried out by different and clearly identifiable persons, and must be supported by a maker and checker mechanism.

- Control activities:
  - The internal set of rules also defines the procedures according to which the disbursement of donations to charities and sponsorships must be preceded by a due diligence process, particularly insofar as the provisions set forth in the Anti-Corruption Guidelines are concerned to be carried out by the Structure involved. In particular:
    - analysis and verification of the type of organisation and of its statutory objects;
    - verification and approval of all disbursements by the Head of the Structure concerned;
    - verification that total disbursements are established annually and funded from a specific budget approved by the competent Bodies;
  - with regard to sponsorships, proper performance of the agreed service by the sponsored entity shall be verified, by acquiring appropriate documentary evidence of such performance.

Furthermore, the Heads of the Structures concerned must:

- ensure that the list of beneficiaries is kept updated and available at all times, including the value of the disbursements or of the gifts distributed, and the dates/occasions of the donations. This requirement does not apply to "marked" gifts, i.e. those bearing the Bank's logo (such as pens, desk items, etc.), and the standard gifts prepared by the central Structures (for example, for the end of the year);
- regularly check the above-mentioned list to identify any abnormal situations.

- Process traceability including both the electronic and the paper trail:
  - to ensure full traceability of both the documentary trail and of the management process in place for gifts, entertainment expenses, donations to charities and sponsorships, the Structures concerned shall, inter alia, prepare reports on disbursements made/contracts entered into;
  - in order to allow reconstruction of responsibilities and the reasons for the choices made, the Structure from time to time concerned shall be responsible for filing and storing, also in telematic or electronic format, all the documentation it produced in performance of the requirements relating to management of gifts, entertainment expenses, donations to charities and sponsorships.

Rules of Conduct

While expenses for gifts are allowed, provided they are of limited value and, in any case, not such as to compromise the integrity and reputation of either of the parties and not such as to influence the beneficiary's independent judgement, the Bank's structures, howsoever involved in the management of gifts, entertainment expenses, donations to charities and sponsorships are required to comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and any provisions of the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines. Specifically:

- the Bank may make disbursements in the form of donations to charities or sponsorships to support the initiatives of lawfully established entities whose activities are not in conflict with the Bank's ethical principles and, in the case of donations for charity, these entities cannot operate on a for profit basis;
- any initiatives falling under one of the categories eligible for "sponsorships" cannot at the same time benefit from charitable contributions;
- the donations shall be paid into a current account held by the beneficiary entity exclusively; payment in cash or to a country other than that of the beneficiary entity or to an individual /entity other than the latter is not allowed.

In any event, it is forbidden to initiate, cooperate/give rise to conduct that could be considered an offence in terms of Legislative Decree 231/2001, and, more specifically by mere way of example, to:

- make disbursements for charity or sponsorship initiatives, in favour of organisations that are party to notorious judicial cases, are engaged in practices involving the infringement of human rights, or contrary to rules on vivisection and environmental protection. No charitable contributions or sponsorships may be given to political parties and movements and their subsidiary organisations, trade unions and welfare associations (patronati), clubs (e.g. Lions, Rotary, etc.), recreational associations and groups, private schools, private schools legally equivalent to public schools and/or legally recognised schools, except for particular initiatives of special social, cultural or scientific value must be approved by the Corporate Anti-Corruption Officer;
- make donations/gifts to entities/members/representatives of the Public Administration, Supervisory Authorities or other public institutions or to other organisations/persons linked to such bodies thereby infringing this protocol and the Anti-Corruption Guidelines;
- promise or pay/offer undue sums of money, gifts, services free of charge (outside the accepted practices of courtesy gifts of little value) or grant advantages or other benefits of any kind – directly or indirectly, for oneself or for others – to members/representatives of the Public Administration, Supervisory Authorities or other public institution or to other organisations in order to further or favour the Bank's interests, also yielding to unlawful pressures. Staff members cannot accept any request for undue benefits or attempts at extortion in office by an official of the Public Administration they might receive or simply become aware of, and must immediately report any such cases to their direct superior, who in turn forwards the report received to the Internal Auditing function and Corporate Anti-Corruption Officer for assessment and the completion of any formalities to the Surveillance Body in accordance with the provisions under paragraph 4.1;
- promise of pay/offer undue sums of money, gifts, services free of charge (outside the accepted practices of courtesy gifts of little value) and grant advantages or other benefits of any nature – directly or indirectly, for oneself or for others – in favour of senior officers or their staff in companies that are counterparties or in relationships with the Bank, in order to unduly favour the interests of the Bank;
- make a gift of goods whose lawful origin has not been verified nor their compliance with the provisions on intellectual property rights, trademark and industrial property right in general and geographic indications and protected designations of origin.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.2.2.10. Management of the staff selection and recruitment process

Introduction

This protocol applies to all the Bank Structures involved in the management of the staff selection and recruitment process.

The process could constitute a possible instrument for the commission of "*Corruption against the Public Administration*", in its various forms, "*Illegal inducement to give or promise benefits*", "*Trafficking of illegal influences*"[26], as well as offences of "*Private-to-private corruption*" and "*Instigating private-to-private corruption*" (described in Chapter 7.4).
This because non-transparent management of the staff selection and recruitment process could allow the commission of such offences through the promise of hiring made to representatives of the Public Administration and/or senior officers and/or their staff in companies or entities that are counterparties or in relationships with the Bank, or to persons indicated by them, in order to influence their independence of judgement or to ensure any benefit for the Bank.

There is also the risk of commission of the offence of the "Employment of foreign nationals with irregular permits of stay".

The definitions given in this protocol are aimed at ensuring the Bank's compliance with applicable regulations and principles of transparency, correctness, objectivity and traceability in carrying out the activities concerned.

Process description

The staff selection and hiring process comprises the following steps:

- Staff selection:
  - needs analysis and request for new hirings;
  - identification of the required candidate profile;
  - recruitment of candidates;
  - candidate selection;
  - choice of the candidates to be hired.

[26] As already stated, under Article 322-*bis* of the Criminal Code, the conduct of the bribe-giver, instigator or person accepting illegal inducement is a punishable criminal offence not only when it involves Public Officials and Public Service Providers within the Italian Public Administration, but also when it involves: i) persons holding corresponding functions or performing corresponding activities within EU institutions, or within Entities established on the basis of the Treaties establishing the EU, or, lastly, within the other European Union Member States; ii) individuals performing corresponding functions or activities in other foreign states, international or supranational public organisations, international parliamentary assemblies or international courts.

- Formalisation of hiring.

The Company Structures so empowered shall directly handle the selection and hiring process concerning specialised and highly qualified staff or top managers (direct hiring).
The operating methods for managing the process are governed as part of internal regulations developed and updated by the competent Structures, which constitute an integral and substantial part of this protocol.

Control principles

The control system for monitoring the processes described above must be based on the following elements:

- Expressly defined authorisation levels:
  - the staff selection and recruitment process is centrally managed by the competent Structure which receives formal requests for the hiring of new staff from the Structures concerned and assesses them consistently with the budget and internal development plans;
  - authorisation to hiring new personnel can only be given by duly empowered staff expressly empowered under the current power and delegation system;
  - the candidates judged to be suitable and whose hiring has been authorised are then hired by the competent Organisational units within each Structure.

- Segregation of duties between the different persons involved in the process. In particular, the final approval of the hiring is issued by different structures, chosen in accordance with the importance of the position to be filled within the corporate organisation.

- Control activities:
  - during the selection process, each candidate has to fill specific forms, to ensure that the candidates' details are collected in a uniform manner;
  - the actual hiring must be preceded by adequate due diligence particularly with regard to the provisions of the Anti-Corruption Guidelines..

- Process traceability including both the electronic and the paper trail:
  - in order to allow reconstruction of responsibilities and the reasons for the choices made, the Structure from time to time concerned shall be responsible for filing and storing, also in telematic or electronic format, all the documentation it produced (including standard documents such as tests, application forms, employment contracts, etc.) relating to performance of the requirements in the course of the staff selection and hiring process.

Rules of Conduct

The Bank's structures howsoever involved in management of the staff selection and hiring process, shall comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and any relevant provisions of the Code of Ethics, the Group's Internal Code of Conduct and Anti-Corruption Guidelines.

Specifically:

- staff members cannot accept any request for undue benefits or attempts at extortion in office by an official of the Public Administration they might receive or simply become aware of, and must immediately report any such cases to their direct superior, who in turn forwards the report received to the Internal Auditing function and Corporate Anti-Corruption Officer for assessment and the completion of any formalities to the Surveillance Body in accordance with the provisions under paragraph 4.1;
- the selection must be made from a shortlist of candidates, except in the case of specialised, qualified staff that is included in protected categories or individuals to be hired for managerial positions;
- the comparative assessment of the candidates must take place on the basis of the criteria of skill, professionalism and experience in relation to the position in question.
- if the hiring process concerns:
  - disabled staff, the recruitment of candidates is arranged from lists of persons in protected categories to be requested from the relevant Employment Office;
  - foreign workers, the process must guarantee compliance with the immigration laws of the country in which the recruiting organisational unit is based and verification of possession of residence permits, where applicable, for the entire duration of the employment contract;
  - former public employees, the process must guarantee compliance with legal restrictions.
- if third parties are to be involved in the management of the staff selection and hiring process, the contracts entered into with such persons shall contain a specific declaration that they know the provisions of Legislative Decree 231/2001, the provisions of the law against corruption and undertake to comply with them;
- the payment of fees or compensation to external collaborators or consultants involved is subject to permission given in advance by the organisational unit responsible for assessing service quality and the resulting fairness of the fee demanded; in any case, no remuneration shall be payable to employees or external consultants where not fully justifiable by the type of work performed or to be performed.

In any case, it is forbidden to engage in, collaborate with or induce conduct which may belong to one of the types of offences covered by Legislative Decree 231/2001; more specifically, purely by way of example and without limitation it is forbidden to:

- promise to hire, or accede to requests to hire representatives/members of the Public Administration or persons indicated by them, in order to influence their independence of judgement or to induce them to grant the Bank any advantages;
- promise to hire, or accede to requests to hire senior officers of their staff in companies that are counterparties or in relationships with the Bank or persons indicated by them, in order to unduly favour the pursuit of the Bank's interests.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.2.2.11. Management of real estate assets and cultural assets

Introduction

The management of real estate assets and cultural assets - meaning all moveable and immovable assets pursuant to Legislative Decree 42/2004[27] concerns any type of activity carried out by the Bank's structures aimed at enhancing and optimising the real estate assets – both owned and leased – and at enhancing, planning actions for and managing the Bank's cultural assets. It includes the possible use for social and / or cultural purposes of real estate and cultural assets of the Bank, as regulated by specific internal rules.

Under Legislative Decree 231/2001, this process could be means for committing the offences of "*Corruption against the Public Administration*" in its various forms, of *"Illegal inducement to give or promise benefits*" and of "*Trafficking of Illegal Influences*"[28] as well as the risk of commission of the offence of "*Private-to-private corruption*" and "*Instigating private-to-private corruption*", described in paragraph 7.4.

This because non-transparent management of the process relating to the management of the Bank's real estate and cultural assets could enable the commission of such offences, through the giving/granting of advantages to members of the Public Administration and/or senior officers and/or their staff in companies or entities that are counterparties or in relationships with the Bank, in order to further the Bank's interests.

There is also a risk of committing offences against cultural and landscape heritage, which involve the administrative liability of the organization in relation to the commission of the offences of the *"Theft of cultural assets", "Misappropriation of cultural assets", "Illegal import of cultural assets", "Unlawful outflows or exports of cultural assets", "Laundering of cultural assets", "Destruction, dispersion, deterioration, disfigurement, dirtying and unlawful use of cultural and landscape assets", "Forgery of works of art", "Receipt of stolen cultural assets", "Forged written documents regarding cultural assets", "Laundering of cultural assets" and the "Destruction and looting of cultural and landscape assets",* described in paragraph 7.7.

The corporate entities in charge of managing documentation to obtain authorizations/certifications/favourable opinions issued by the Public Administration, must comply

[27] Pursuant to Article 2 of the Code of cultural and landscape assets, cultural assets refer to those assets (moveable items and real estate of artistic, historic, archaeological, ethno-anthropological, archive and bibliographic interest and other items identified by laws or based on laws which reflect the value of civilisation (pursuant to Articles 10 and 11) and that have a value in terms of the landscape (real estate and the areas indicated in Article 134, that reflect the historic, cultural, natural, morphological and aesthetic values of the territory, and other items identified by law or based on law).

[28] As already stated, under Article 322-*bis* of the Criminal Code, the conduct of the bribe-giver, instigator or person accepting illegal inducement is a punishable criminal offence not only when it involves Public Officials and Public Service Providers within the Italian Public Administration, but also when it involves: i) persons holding corresponding functions or performing corresponding activities within EU institutions, or within Entities established on the basis of the Treaties establishing the EU, or, lastly, within the other European Union Member States; ii) individuals performing corresponding functions or activities in other foreign states, international or supranational public organisations, international parliamentary assemblies or international courts.

with the rules of conduct set out and described in the protocol "*Management of activities relating to requests for authorization or fulfilment of requirements towards the Public Administration*".

The contents of this protocol are aimed at ensuring that the Bank complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in the performance of the activity in question.

Process description

The management of the Bank's real-estate and cultural assets comprises the following processes:

Management of the real-estate assets:

- administrative and accounting management of the real estate properties;
- managing the lease / loans for use contracts;
- managing running expenses and tax charges.
- identifying and selecting investment /disposal opportunities;
- purchasing and selling the real estate properties;
- optimising the real estate assets currently held;
- planning the Bank's long term real estate strategy;
- design, maintenance and execution of the works.

Management of cultural assets (Movable assets and real estate and protected decorative items[29]):

- acquiring assets from corporate transactions (mergers, incorporations), donations, market acquisitions;
- managing loan/lease/loan-for-use contracts;
- sale, also not for a consideration;
- managing activities concerning inspections, registration, retention, maintenance and related obligations with the Public Administration;
- managing incidents (loss, theft, deterioration, damage, destruction, misuse).

The operating procedures for management of the processes are governed by the internal rules, which are developed and updated by the competent Structures, and which form an integral and substantive part of this protocol.

[29] As regards real estate and decorative items that are part of a cultural assets, reference is also made to the above processes on property management

Control principles

The control system for monitoring the processes described above must be based on the following elements:

- Expressly defined authorisation levels. Specifically:
  - persons exercising authorisation and/or negotiating powers in the management of real-estate and cultural assets :
    - are identified and authorised on the basis of their specific role assigned by the organisational code or by Head of the reference Structure by means of internal delegation, to be kept on file by the same Structure;
    - only operate within the scope/portfolio of customers assigned to them by the Head of the reference Structure;
  - all the decisions relating to purchases and sales, sale without a consideration, leases and concessions on loans for use and loans shall be taken exclusively by persons duly empowered under the current power and delegation system, which sets out the level of decision-making autonomy according to type and amount of expenditure. The internal set of rules illustrates these authorisation mechanisms and indicates the corporate officials who hold the necessary powers.

- Segregation of duties between the different persons involved in the process. Specifically:
  - the activities relating to the different phases of the process must be carried out by different and clearly identifiable persons and must be supported by a maker and checker mechanism.

- Control activities:
  - checking the appropriateness of the lease payments to be made or received for all new lease contracts or contract renewals, having regard to current market prices or in compliance to the provisions of a public bidding procedure;
  - checking that the purchase/sale price is in line with market levels, also by commissioning independent experts' reports each time the counterparty is a Public Administration or one of its members and/or senior officers and/or their staff of companies that are counterparties or in relationships with the Bank;
  - performing a due diligence on the contractual counterparty particularly with regard to the provisions of the Anti-Corruption Guidelines;
  - verifying in detail all the data contained in the purchase and sale contracts and, in particular, checking the consistency between the preliminary sale agreement and the final agreement;
  - preparing and updating the register of current leases and loans for use, with detailed entries for new relationships and those renewed in the reference period;
  - preparing and updating the register of movable property of cultural value and classified documentation in historic archives;
  - for goods intended for initiatives with social and / or cultural purposes subject to loan for use, loans, sale without a consideration, lease or sale:

- carrying out the due diligence of the beneficiary aimed at:
  - analyzing the type of institution and the purpose for which it was created;
  - checking the reliability and reputation of the beneficiary institution, with particular attention to criminal records and/or charges;
  - verifying whether the beneficiary institution meets the requirements for operating in accordance with the provisions of applicable law to the beneficiary institution;
  - identifying any risks which may be associated with the beneficiary institution;
- verify that the act contains appropriate contractual precautions so that the asset remains for a reasonable period of time in the availability of the beneficiary institution and that it is not possible to change its intended use and / or social and / or cultural purpose
- no need to verify the adequacy of the fee or price with respect to market conditions;

- verify for all purchased cultural assets, that the following exist:
  - a report of an independent expert certifying the legal origin and authentic nature of the cultural assets or a statement from the Superintendent of Archive and Bibliographic Material certifying the particularly important historic interest of archive material;
  - a report on protected real estate, indicating direct constraints;
- verify, at the time of the sale, also without a consideration, of the Bank's cultural assets, the existence of the report or statement of the Superintendent of Archive and Bibliographic Material as above, the authorisation required, the correct management of reporting information to the competent Authorities and compliance with pre-emption terms in favour of the Ministry, or as applicable, the Region or another local public organisation concerned;
- verify, in the case of the transfer of movable goods belonging to the Bank's cultural assets abroad, the existence of the free transit declaration or export licence;
- verify that authorisation required by the competent Authorities has been obtained before proceeding with works on assets subject to cultural or landscape constraints.

- Process traceability including both the electronic and the paper trail:
  - each major phase of dispositions (purchase and sales, leases, sale even without a consideration, loans for use) must be recorded in specific written documents;
  - each disposition (purchase and sales, leases, loans for use, loans and sale even without a consideration) shall be formalised in a document, which shall be duly signed by persons holding the required powers under the current power and delegation system;
  - in order to allow reconstruction of responsibilities and the reasons for the choices made, the Structure from time to time concerned shall be responsible for filing and storing, also in telematic or electronic format, all the documentation it produced relating to performance of the requirements relating to management of the real estate and cultural assets.

- Bonus or incentive systems: bonus and incentive systems must be able to guarantee compliance with legal provisions, the principles of this protocol and the provisions of the Code of Ethics, also envisaging suitable corrective mechanisms for any conduct deviating from the norm.

Rules of Conduct

All the departments involved in management of the Bank's real-estate and cultural assets shall comply with the procedures set out in this document, the applicable provisions of the law, the internal rules and any provisions of the Code of Ethics, the Group's Internal Code of Conduct and Anti-Corruption Guidelines.

Specifically:

- persons exercising authorisation and/or negotiating powers must be identified and authorised on the basis of their specific role assigned by the organisational code or by Head of the reference Structure by means of internal delegation, to be kept on file by the same Structure;
- the granting of goods intended for initiatives with social and / or cultural purposes must be carried out to support the initiatives of lawfully established Entities whose activities are not in conflict with the Bank's ethical principles and these Entities cannot operate on a for profit basis;
- staff members cannot accept any request for undue benefits or attempts at extortion in office by an official of the Public Administration they might receive or simply become aware of, and must immediately report any such cases to their direct superior, who in turn forwards the report received to the Internal Auditing function and Corporate Anti-Corruption Officer for assessment and the completion of any formalities to the Surveillance Body in accordance with the provisions under paragraph 4.1;
- if third parties are to be involved in the management of the Bank's real-estate and cultural assets, the contracts entered into with such persons shall contain a specific declaration that they know the provisions of Legislative Decree 231/2001, the provisions of the law against corruption and undertake to comply with them;
- the payment of fees or compensation to external collaborators or consultants involved is subject to permission given in advance by the organisational unit responsible for assessing service quality and the resulting fairness of the fee demanded; in any case, no remuneration shall be payable to employees or external consultants where not fully justifiable by the type of work performed or to be performed;
- the theft, loss, deterioration, damage, destruction and misuse - or use that harms the conservation - of the Bank's cultural assets shall immediately be notified as indicated in internal rules.

In any case, it is forbidden to engage in, collaborate with or induce conduct which may be instrumental to commission of one of the types of offences covered by Legislative Decree no. 231/2001; more specifically, purely by way of example and without limitation it is forbidden to:

- present incomplete documents and data and/or communicate false or altered data;
- use deceit which could lead Public Entities in error;
- create, wholly or in part, false documents or, alter, destroy, eliminate or conceal a true document, in relation to cultural assets in order to make their origin appear to be lawful;
- promise or supply real-estate and cultural assets – also through intermediaries - to Public Administration Bodies, public institutions or persons indicated by them on non-market conditions,

without prejudice to cases of concession of goods intended for initiatives with social and / or cultural purposes as regulated by specific internal rules;

- promise or supply real-estate and cultural assets to senior officers and/or their staff in companies that are counterparties or in relationships with the Bank, or to persons indicated by them, in order to unduly favour pursuit of the interests of the Bank;
- grant, in the context of initiatives with social and / or cultural purposes, real-estate and cultural assets in favor of Entities that are party to notorious judicial cases, are engaged in practices involving the infringement of human rights, or contrary to rules on vivisection and environmental protection. Said entities cannot be recipients of the concession of such goods political parties and movements and their subsidiary organisations, trade unions and welfare associations (patronati), clubs (e.g. Lions, Rotary, etc.), recreational associations and groups, private schools, private schools and/or legally recognised schools, except for particular initiatives of special social, cultural or scientific value must be approved by the Corporate Anti-Corruption Officer;
- authorise the payment of invoices payable without having carefully and thoroughly checked the stated amount payable;
- award appointments to external consultants without following substantiated and objective criteria addressing professionalism and expertise, competitiveness, price, integrity and the ability to provide effective assistance. In particular, the rules for the selection of consultants shall refer to the criteria of clarity and availability of documentary evidence laid down in the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines; this is in order to prevent the risk of bribery offences, in their various forms, of "*Illegal inducement to give or promise benefits*", and of "*Trafficking of illegal influences*", which could result from the selection of individuals who are "close" to persons linked to the Public Administration and thus the possibility of facilitating or influencing the management of contractual relations with the Bank
- transfer movable goods belonging to the Bank's cultural assets abroad, without the free transit declaration or export licence;
- place in circulation, as authentic, counterfeit, altered or reproduced specimens of movables belonging to the Bank's cultural assets.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.2.2.12. Management of relations with regulatory bodies

Introduction

This protocol applies to all the Bank Structures involved in the management of relations with the Supervisory Authorities, and concerns all types of activity implemented in respect of remarks, requirements, communications, requests and inspections. This also includes advocacy services or the preparation of opinions, proposals and replies to consultations on regulations already existing, or about to be introduced. Refer to protocol 7.2.2.7. with regard to relations with the Supervisors.

Pursuant to Legislative Decree 231/2001, this process could present opportunities for committing the offences of "*Corruption against the Public Administration*" in its various forms, of "*Illegal inducement to provide or promise benefits*", and "*Trafficking of illegal influences*"[30].

The contents of this protocol are aimed at ensuring that the Bank complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in the management of relations with:

- all Italian and international institutions, including but not limited to the Italian parliament, local governments, the Government, the Bank of Italy, the AGCM, the OAM, the OCSF, CONSOB and the Data Protection Authority, foreign governments or parliaments, regulatory bodies in countries which are relevant to the activities of the Bank and of the Group;
- all international and multilateral institutions, including but not limited to EC institutions (the European Commission, the Council of the European Union and the European Parliament), the European Supervisory Authorities ("ESAs"), the European Central Bank, the European Data Protection Board ("EDPB"), the Basel Committee for Banking Supervision ("BCBS"), the Financial Stability Board ("FSB"), the World Bank ("WB") and the International Monetary Fund ("IMF");
- the trade associations, think tanks and interest groups in which the Bank and Group participate with or without permanent representatives, in order to set up – in line with the principles on the safeguarding of competition - discussion groups with other market players or stakeholders of the Bank or Group for the preparation of opinions, proposals or replies to consultations on existing or future regulations.

[30] As already stated, under Article 322-*bis* of the Criminal Code, the conduct of the bribe-giver, instigator or person accepting illegal inducement is a punishable criminal offence not only when it involves Public Officials and Public Service Providers within the Italian Public Administration, but also when it involves: i) persons holding corresponding functions or performing corresponding activities within EU institutions, or within Entities established on the basis of the Treaties establishing the EU, or, lastly, within the other European Union Member States; ii) individuals performing corresponding functions or activities in other foreign states, international or supranational public organisations, international parliamentary assemblies or international courts.

Process description

Activities relating to the management of relations with the supervisory authorities, either directly or through third parties (consultants, trade associations, think tanks and interest groups) are as follows:

- contact with the Entity;
- compliance with specific requests/consultation documents;
- the production of specific demands or position papers;

The "Group Rules on the management of relations with regulators and supervisory authorities" identify the Bank departments tasked with coordinating the communications between these authorities and with ensuring that these communications are consistent at Group level (Pivot Structure).

The Pivot Structure will involve the "Functional Owners" on aspects or for contributions pertaining to their respective areas, depending on the object or scope of the contract or issue in question.

The operating methods for managing the process are governed as part of internal regulations developed and updated by the competent Structures, which constitute an integral and substantial part of this protocol.

Control principles

The control system for monitoring the process described above must be based on the following elements:

- Expressly defined authorisation levels. Specifically:
  - relations with the regulators are undertaken by the head of the relevant department, or by people who are identified and authorised according to the specific role given to them in the organisational chart, or by individuals identified by the head of the relevant department, through an internal delegation which is kept by that department;
  - all acts which involve a contractual commitment on the part of the Bank must be signed solely by duly appointed persons.

- Segregation of duties between the different persons involved in the process. In particular, advocacy activities are performed by departments other than those directly affected by the regulation in question.

- Control activities:
  - controls concerning the completeness, correctness and accuracy of the information provided to the Supervisory Authorities by the Structure concerned as to the activities falling under its competence that must be supported by maker and checker mechanisms;

- verification of compliance with the criteria laid down in company regulations regarding the selection of suppliers and professionals (before the relationship is established, due diligence must be carried out with particular regard to the requirements of the Anti-corruption Guidelines).

- Process traceability including both the electronic and the paper trail:
  - each key phase of the process must be recorded in writing;
  - To enable a clear understanding of the responsibilities and the motives behind the choices made, the Structure from time to time involved shall be responsible for archiving and preserving the documentation produced also by electronic means, in relation to the management of relations with regulatory bodies.

Rules of Conduct

The Bank Structures howsoever involved in the management of relations with the Supervisory Authorities shall comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and any provisions of the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines.

Specifically:

- the persons involved in the process that are responsible for signing acts or documents which are relevant outside the Bank must be expressly appointed;
- staff members cannot accept any request for undue benefits or attempts at extortion in office by an official of the Public Administration they might receive or simply become aware of, and must immediately report any such cases to their direct superior, who in turn forwards the report received to the Internal Auditing function and Corporate Anti-Corruption Officer for assessment and the completion of any formalities to the Surveillance Body in accordance with the provisions under paragraph 4.1;
- staff must provide the Authorities with accurate, truthful, correct and up-to-date information, and must differentiate facts from opinions; they must not present information in a way that could give rise, even potentially, to confusion, misunderstanding or error on their part;
- staff must unequivocally declare any existing or potential conflict of interest in advance, to the Authorities;
- if third parties are to be involved in the handling of relations with the regulators or with the public administration in general, the contracts entered into with such persons shall contain a specific declaration that they know the provisions of Legislative Decree 231/2001 and undertake to comply with them;
- the payment of fees or remuneration to any service providers involved is subject to prior authorisation to be issued by the organisational unit which is competent to assess the quality of service and the consequent appropriateness of the remuneration requested; in any case, no remuneration shall be payable to service providers where it is not adequately justified by the type of work performed or to be performed.

In any event, it is forbidden to initiate, cooperate/give rise to conduct that could be considered an offence in terms of Legislative Decree 231/2001, and, more specifically by mere way of example, to:

- ask or induce representatives of the regulators or the public administration in general to grant preferential treatment;
- promise or pay/offer undue sums of money, gifts or free benefits (apart from courtesy gifts of low value) or grant advantages or other benefits of any kind – directly or indirectly, on one's own behalf or for others − to representatives of the regulatory bodies or of the Public Administration in order to further or favour the Bank's interests. Examples of such improper advantages include, without limitation, the promise to hire family members and relatives, disbursement of credit under terms not compliant with the principles of sound and prudent management envisaged in company regulations, all banking or financial transactions which generate a loss for the Bank and a profit for the aforementioned persons (e.g. unjustified cancellation of a debt position and/or application of discounts or conditions not in line with market parameters);
- award appointments to external consultants without following substantiated and objective criteria addressing professionalism and expertise, competitiveness, price, integrity and the ability to provide effective assistance. In particular, the rules for the selection of consultants shall refer to the criteria of clarity and availability of documentary evidence laid down in the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines; this is in order to prevent the risk of corruption offences, in their various forms, and of the offence of "*Illegal inducement*" offences or of "*Trafficking of illegal influences*", which could result from the selection of individuals who are "close" to persons linked to the regulatory bodies or to the Public Administration and thus give rise to the possibility of facilitating or influencing the management of contractual relations with the Bank.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.3 Sensitive area concerning the counterfeiting of money (and valuables)

7.3.1 Offences

Introduction

Article 25-*bis* of the Decree covers a series of offences listed in the Criminal Code, the aim being to protect public trust, which is society's reliance on the genuineness and integrity of certain specific symbols, which is essential to ensure the safe and timely performance of economic exchanges. The criminal conduct punished concerns coins, banknotes, cards and bearer's coupons issued by Governments or authorised Institutes – official stamps, watermark paper and instruments or objects intended for counterfeiting currency[31].

In particular, the following types of crimes are identified.

Counterfeiting money, spending and introducing counterfeit money into the country, in conspiracy with others (Article 453 of the Criminal Code)

Altering money (Article 454 of the Criminal Code)

Counterfeiting of money occurs when a person manufactures counterfeit money, whereas altering, which is a different offence, consists of making money appear to have a higher value than its true one.

In both types of offences, the law punishes both the author of the counterfeiting or the altering, and the person that, in cooperation with the author of the counterfeiting or altering, or with an intermediary of such person, introduces into the territory of the State, holds or howsoever puts into circulation the money thus counterfeited or altered; lastly, the law also punishes any person that obtains such counterfeit or altered money in order to put it into circulation, from either the author of the counterfeiting or alteration or from his intermediary.

The possibility that bank staff members might engage in the altering or counterfeiting of money, alone or in conspiracy with others in the bank's own interest seems highly unlikely; greater risks may concern the offence of circulating the counterfeit currency and receiving it order to put it into circulation.

Spending and introducing counterfeit money into the country, not in conspiracy with others (Article 455 of the Criminal Code)

Unknowingly passing counterfeit money (Article 457 of the Criminal Code)

[31] Law 99/2009 amended Article 25-bis, adding to currency counterfeiting offences the counterfeiting of trademarks, distinctive signs, patents and models (Articles 473 and 474 of the Criminal Code), which are covered in section 7.10 of this document.

The type of offence covered by Article 455 of the Criminal Code, which is much rarer than those covered by the two preceding Articles, assumes in any case that the person engaging in the conduct was aware or suspected from the start that the coins were not authentic, despite the lack of any agreement with the person that falsified them.
In the types of offences referred to in Article 457 of the Criminal Code, on the contrary, the essential and distinctive element is the initial good faith of the person that engages in the criminal conduct; this good faith only ceases at the time of spending or, in general, of putting into circulation the counterfeit or altered currency.
This offence might therefore apply to a bank teller who uses counterfeit banknotes for transactions with customers, also where he has received them in good faith, in order to prevent the bank from incurring damage or quite simply to avoid the problems inherent in acknowledging and reporting the counterfeit nature of the banknotes.

Counterfeiting official stamps, introducing into the country, purchasing, possessing or circulating counterfeit official stamps (Article 459 of the Criminal Code)
Counterfeiting of watermark paper for producing banknotes or official stamps (Article 460 of the Criminal Code)
Making or possessing watermarks or instruments for the purpose of counterfeiting money, official stamps or of watermark paper (Article 461 of the Criminal Code)
Using counterfeit or altered official stamps (Article 464 of the Criminal Code)
In the light of the peculiar character of the material subject of the offences in question, the likelihood that such offences might be committed by bank staff seems to be very remote.

7.3.2 Sensitive company activities

The sensitive activity identified by Model where the risk for money counterfeiting offences is highest is the following:

- Management of valuables.

We reproduce below the protocol laying down the control principles and rules of conduct applicable to this activity, as well as the detailed corporate regulations governing this activity.

Such protocols also apply to the monitoring of any activities performed by Group companies or outsourcers on the basis of special service agreements.

7.3.2.1. Management of valuables

Introduction

The management of valuables includes all activities relating to the handling of valuables of any kind, with particular reference to banknotes, coins and official stamps which are legal tender in Italy and abroad.

Pursuant to Legislative Decree 231/2001, the related process might offer opportunities for commission of the offences of "*Counterfeiting money, spending and introducing counterfeit money into the country, in conspiracy with others*" (Article 453 of the Criminal Code), "*Altering money*" (Article 454 of the Criminal Code), "*Spending and introducing counterfeit money into the country, not in conspiracy with others*" (Article 455 of the Criminal Code), and "U*nknowingly passing counterfeit money*" (Article 457 of the Criminal Code).

Although the Bank's traditional activity is centred on the management of the valuables, the likelihood that Bank staff would, alone or in conspiracy with others, and acting in the Bank's interest engage in the altering or counterfeiting of valuables seems remote.

A higher level of risk might concern, on the other hand, the putting into circulation of counterfeit and/or altered valuables, since the Bank may incur administrative liability where, while not conspiring with the authors of the counterfeiting, a bank employee, who doubts the authenticity of certain valuables on receiving them, but is not absolutely sure of their being counterfeit, puts them into circulation in order to prevent the Bank from incurring damage or quite simply avoiding the problems inherent in recognising and reporting the falsity of the valuables to the competent Authorities.

The definitions given in this protocol are aimed at ensuring the Bank's compliance with applicable regulations and principles of transparency, correctness, objectivity and traceability in carrying out the activities concerned.

Process description

The process involves the following phases:

- handling of the valuables (cashier's transactions, night safe, ATM / ATM operation, transfer of valuables to the Branches and payments to the Bank of Italy, external transactions);
- monitoring and examination of the valuables;
- management of the valuables and in particular of any suspicious banknotes (withdrawing the banknotes, preparing a report, submitting the report and the banknotes to the competent Authorities and filing the documentation).

The operating procedures for management of the process are governed by the internal rules, which are developed and updated by the competent Structures, and which form an integral and substantive part of this protocol.

Control principles

The control system for monitoring the process described above must be based on the following elements:

- Expressly defined authorisation levels. Specifically:
  - persons involved in the process of handling valuables shall be identified and authorised by the Head of the reference Structure by means of an individual assignment of the devices to be moved and/or the safeguarding of the securities themselves and these assignments shall be indicated in specific operating processes;
  - the conclusion of contractual relationships with intermediaries tasked with processing of the valuables must be authorised by persons duly empowered under the current power and delegation system.

- Segregation of duties between the different persons involved in the process.

- Control activities: the reference internal regulation identifies the line controls that must be performed by each Structure/Branch concerned when handling valuables relating to performance of the process subject of this protocol. Specifically:
  - on an annual basis, the Structure concerned verifies:
    - valuables handled by Branch operators (cash, blank valuables, other valuables) in order to ascertain the accounting position and real stock of cash valuables;
    - practices adopted by the Branch after the discovery of banknotes and coins suspected to be false, in order to ascertain the correct implementation of operating rules envisaged in the most recent internal regulations;
  - with reference to the night safe/collection of valuables through intermediaries, the opening of the armoured equipment and the checks on the containers and the valuables must be performed by two employees working together without interruption;
  - with reference to the management of ATMs, the opening of the armoured vehicle, uploading of banknotes, checking of the valuables, recovery of debit cards captured by the machine and clearance of accounts must be done by two employees working together at all times. In exceptional or unavoidable situations, the system allows for the operations to be performed by a single operative, with provision for joint checking at a later time, in accordance with the internal regulations;
  - the Head of the Structure/Operating Point Manager, or an employee designated by them shall, at least once a quarter carry out spot checks on the quantitative and qualitative content of the wads being delivered, recording the checks carried out and their results.

- Process traceability including both the electronic and the paper trail:
  - in implementing the operations required for putting valuables into circulation, supporting IT systems shall be used to ensure traceability of the operations performed;

- in order to enable reconstruction of responsibilities, the Structure from time to time concerned shall be responsible for filing and storing, also in telematic or electronic format, all the documentation it produced in performing activities associated with the process of managing the valuables, including the transfer of suspicious banknotes to the Bank of Italy.

Rules of Conduct

The Bank's structures howsoever involved in the management of valuables shall comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and any provisions of the Group's Code of Ethics and Internal Code of Conduct.

In particular all persons whose duties include the handling of valuables for whatever reason:

- must be specifically authorised in the specific operating procedures;
- have an obligation to operate with honesty, integrity, correctness and good faith;
- have an obligation to pay special attention to dealings with customers who are not sufficiently known to them, or to transactions concerning substantial amounts;
- must thoroughly check the valuables they receive, in order to identify any suspicious valuables. For identification purposes, banknote selection and acceptance equipment may also be used, making it possible to check both the banknotes' authenticity and their suitability for circulation, or only their authenticity; alternatively, the authenticity checks can be carried out by trained staff, by means of manual checks without using selection and acceptance devices;
- must, where they detect banknotes which they suspect of being counterfeit,
  - promptly prepare a report of withdrawal from circulation of such suspicious banknotes and report the finding to the competent Authority (Central Means of Payment Antifraud Office - UCAMP, Bank of Italy) in accordance with the procedures and time limit set out in the internal regulation;
  - must hold the banknotes suspected of being counterfeit and for which the specific report was prepared in appropriate safes for the period between the date of detection/withdrawal of the banknote from circulation up to its forwarding to the Bank of Italy;
  - must immediately report to their superior any attempt to circulate banknotes or valuables suspected of being counterfeit on the part of customers or third parties and of which the staff was the target or simply became aware of. The superior shall in turn forward the report received to the Internal Auditing Structure for appropriate assessment and the completion of any formalities to the Surveillance Body in accordance with the provisions under Chapter 4.1.

Furthermore:

- if third parties are to be involved in the handling of valuables, the contracts entered into with such persons shall contain a specific declaration that they know the provisions of Legislative Decree 231/2001 and undertake to comply with them;
- the payment of fees or remuneration to any service providers involved is subject to prior authorisation to be issued by the organisational unit which is competent to assess the quality of service and the consequent appropriateness of the remuneration requested; in any case, no

remuneration shall be payable to service providers where it is not adequately justified by the type of work performed or to be performed.

In any event, it is forbidden to initiate, cooperate/give rise to conduct that could be considered an offence in terms of Legislative Decree 231/2001, and, more specifically by mere way of example, to:

- put valuables into circulation, alone or in conspiracy with others. An employee who receives a banknote in good faith and subsequently suspects it of being counterfeit, shall not attempt to put such suspicious banknote back into circulation or to return it to the person that gave it to him, cut it in half or destroy it;
- infringe the provisions of the current rules and legislation on the withdrawal from circulation and forwarding to the Bank of Italy of the euro denominated banknotes suspected of being counterfeit.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.4 Sensitive area concerning corporate offences

7.4.1 Offences

Introduction

Article 25-*ter* of the Decree covers almost all corporate offences envisaged in Title XI of the Civil Code that qualify as general offences, in that they are not specifically referable to the exercise of banking activity[32].

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

With regard to the types of criminal offences in respect of accounting documents and the controls to be performed by the Supervisory Authorities, it should be noted that the Bank – also in its capacity as a listed company – is well placed to put in place effective prevention measures to soundly implement legislative provisions, as it is governed by special legislation requiring it to formalise the whole process of preparing accounting reports, and it must fulfil a series of obligations and requirements towards the Authorities. As a consequence, the procedures for managing the risk of offences outlined in this document reflect actions which are already well established in banking practice, or which derive in any way from the application of the primary legislation and regulation in force.

The types of offences cited by Article 25-*ter* of the Decree are listed below.

False corporate reporting (Article 2621 of the Civil Code)

False corporate reporting by listed companies (Article 2622 of the Civil Code)

These offences are committed by conduct which, with reference to the view of the profit and loss, balance sheet or cash flow situation of the Company or of the Group it belongs to, consist in the knowledgeable

- presentation of untrue material facts in the financial statements, reports or other corporate disclosures addressed to the shareholders or the general public

[32] Article 25-*ter* was amended by:
- Law 190/12 that added the reference of the new offence of "*Private-to-private corruption*" envisaged in Article 2635, paragraph 3, of the Civil Code, which entered into force on 28 November 2012;
- Law 69/15, that eliminated references to conditions for liability of legal entities partially different from the ordinary conditions for corporate crimes and reformed the offences of false corporate reporting with effect from 14 June 2015.

- omission of relevant material facts whose disclosure is required by the law.

In any case, the conduct is a punishable offence when it is carried out for the purpose of unfair gain for the perpetrators or others and is capable of actually leading the intended recipients to err. Furthermore, the illegal act subsists even if it refers to assets held or administered by the company on behalf of third parties.

When the false reporting concerns unlisted companies or those deemed equivalent thereto[33]:

- the presentation of untrue material facts constitutes the offence in question only if it is contained in corporate communications required by law and if the facts are relevant;
- reduced penalties and the grounds for exclusion of liability to criminal punishment applies in particularly exiguous cases[34].

False reports or communications from the independent auditors (Article 27 of Legislative Decree 39/2010)

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

This offence is punished more severely where: it causes financial damage to the recipients of the communications; it concerns the auditing of certain entities defined by the Decree as being "of public interest" (including listed companies, the issuers of financial instruments having wide public circulation, banks, certain insurance companies, stock brokerage companies (SIM), asset management companies (SGR), UCITs, the financial intermediaries referred to in Article 107 of the Banking Law); it is committed in exchange for money or other benefit; it is committed in conspiracy with members of the audited company.

The main offenders in this type of crime are the heads of the independent auditors (offence connected to their office). Also envisaged is the punishment of any person who gives or promises money or benefits, and to the general managers and the members of the administrative organ and of the control body of the public interest entities who aid and abet in commission of the offence.

At present this is not an offence in which corporate liability is presumed[35].

[33] Deemed equivalent to companies listed in a regulated national or European Union market are the companies that control them, companies that are issuers of financial instruments for which admission to trading in said markets has been requested or that are traded on an Italian multilateral trading facility, as well as companies that make public offering transactions, or in any case which manage them.

[34] See Article 2621-*bis* of the Italian Civil Code which provides for a smaller penalty if the facts are of minor entity, in consideration of the nature and size of the company and of the methods or effects of the conduct, or if the facts regard small companies that cannot be subject to bankruptcy proceedings. In the latter case, the offence is prosecutable only through lawsuit. Additionally, Article 2621-*ter* of the Italian Civil Code cites the enforceability of Article 131-*bis* of the Criminal Code that excludes liability to punishment when, due to the methods of the conduct and to the exiguity of the damage, or of the hazard, the offence is particularly exiguous and the conduct is not habitual.

[35] Article 25*ter* of Legislative Decree 231/2001 even now refers to Article 2624 of the Civil Code which originally envisaged this offence, despite regulatory developments in the meantime. Indeed:

- Law 262/2005 introduced Article 174-*bis* of the Finance Consolidation Act, which used a separate instance to punish the inclusion of false information in the audit of listed companies, their subsidiaries and issuers whose financial instruments are widely circulated among the public;

Obstruction of controls (Article 2625 paragraph 2 of the Civil Code)

The offence referred to in Article 2625 paragraph 2 of the Civil Code occurs where the directors conceal documents or otherwise act so as to prevent or hinder performance of the control activities legally vested in the shareholders or other Corporate bodies, thereby causing damage to the shareholders. The offence is prosecutable on the complaint of the injured party, and the sentence shall be harsher if the offence involves a listed company or issuers whose financial instruments are widely circulated among the public.

The case of obstruction of control of an independent auditor, originally also envisaged in Article 2625 of the Civil Code[36], at present does not constitute an offence in which corporate liability is presumed.

Undue repayment of contributions (Article 2626 of the Civil Code)

In its typical form, this offence, apart from cases of lawful share capital reductions, occurs where the shareholders' contributions are returned to them, also by means of simulated transactions, or where the shareholders are exempted from the obligation to make such contributions.

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

This offence consists of distributing profits or advances on profits not actually made, or which under the law should be appropriated to reserves, or of distributing reserves, including those not created through profits, which are legally non-distributable.

It should be noted that returning the profits or re-establishing the reserves before the time-limit specified for approval of the financial statements extinguishes the offence.

Unlawful dealing in the stocks or shares of the company or its parent company (Article 2628 of the Civil Code)

This offence is committed by the purchase or the subscription, apart from the cases permitted by law, of stocks or shares in the company itself or in its parent company, which cause damage to the integrity of the share capital or of non-distributable reserves.

- after reform of statutory auditing regulations, both Article 2624 of the Civil Code and Article 174-*bis* of the Finance Consolidation Act were repealed and, with effect from 7 April 2010, giving false information in audits is punished under the new terms envisaged in Article 27 of Legislative Decree 39/2010.

This development gave rise to serious doubts about the permanent qualification of corporate liability for such conduct. By judgement 34476/2011, the Joint Criminal Chambers of the Court of Cassation decided that the offence of giving false information in statutory audits now envisaged in Article 27 of Legislative Decree 39/2010 no longer falls within the scope of application of corporate administrative liability, in that this ruling is not referred to in Article 25-*ter* of Legislative Decree 231/2001. It should also be considered that certain bribes in relation to auditors are envisaged and punished pursuant to Articles 28 and 30 of Legislative Decree 39/2010, but do not constitute an offence for which corporate liability is presumed.

[36]Article 2625 of the Civil Code also contemplated the offence of obstruction of control of directors in relation to independent auditors. Following the reforms to the rules on the legal auditing of accounts, this offence is no longer governed by Article 2625 civil code. It was reformulated within article 29 of Legislative Decree 39/10 and was then decriminalised in Legislative Decree 8/16; As Article 25-*ter* of Legislative Decree 231/01 was not amended to include a reference to Article 29, it can be said that the offence of impeding the work of the auditing firm is no longer covered by the rules on corporate administrative liability. In this respect the principle indicated in the Court of Cassation judgement referred to in note 30 would seem to apply.

It should be noted that if the share capital or the reserves are restored before the time limit for approval of the financial statements for the period in which the event took place the offence is extinguished.

Transactions prejudicial to creditors (Article 2629 of the Civil Code)

This offence is committed when, in breach of the provisions of the law protecting creditors, reductions in share capital or mergers with other companies or demergers are carried out, such as to cause damage to the creditors.

It should be noted that compensating the creditors for the damage incurred before the judgement is a means of extinguishing the offence.

Failure to disclose conflicts of interest (Article 2629-*bis* of the Civil Code)

This offence occurs where a director or a member of the Board of Directors (where the dual system is adopted) of a company listed on an Italian or EU regulated market or whose shares are widely distributed among the public, or of a company subject to supervision pursuant to the Consolidated Law on Banking, the Consolidated Law on Financial Intermediation or to legislation on insurance activities or supplemental pension funds fails to notify, in the manner and within the deadline set out in Article 2391 of the Civil Code the body he belongs to or the company and in any case the Board of statutory auditors, of any interest they might have personally or on behalf of third parties in a given transaction of the company in question, or, in the case of Managing Director, he does not abstain from carrying out this transaction, thereby causing a damage to the company or to third parties.

Fictitious capital formation (Article 2632 of the Civil Code)

This offence takes place where the directors and shareholders making capital contributions falsely form or increase the company's capital by assigning a number of stocks or shares for an overall value exceeding the amount of the share capital, by mutual underwriting of stocks or shares, by substantially overvaluing contributions made in kind or through receivables or by overvaluing the company's assets in the event of company transformation.

Improper distribution of the company's assets by its liquidators (Article 2633 of the Civil Code)

The offence occurs where the liquidators distribute the company's assets among the shareholders before paying off the company's creditors or before appropriating the sums necessary to satisfy creditors' claims, thereby causing damage to the creditors.

It should be noted that compensating the creditors for the damage incurred before the judgement is a means of extinguishing the offence.

Private-to-private corruption (Article 2635, paragraphs 1 and 3, of the Civil Code)

Instigating private-to-private corruption (Article 2635 *bis*, paragraph 1 of the Civil Code)

The offence of "*Private-to-private corruption*" is any act by the directors, directors general, financial reporting officers, statutory auditors, liquidators or other individuals vested with powers of management within a company or private entity and persons under their management or supervision, who – either directly or through another person, for themselves or for others – solicit or receive cash or other undue benefits, or accept the promise of cash or benefits in order to carry out or omit an act that conflicts with their duties or with their obligations of loyalty towards their company or private entity.

The conduct of the bribe-giver is also punished. This is the person who improperly offers, promises or gives money or other gifts, including through another person.

Punishment for *"Instigating private-to-private corruption"* falls on the person that makes an offer or promise that is not accepted, or the managers of companies or private entities that solicit the gift or promise are punished, if their solicitation is not accepted[37].

Only the conduct of the bribe-giver (offer, gift or promise, whether or not they are accepted), not that of the bribe-takers (acceptance or solicitation), constitute an offence of administrative responsibility, if the offences are committed in the interest of the company/entity the bribe-giver belongs to[38].

Both these offences are automatically subject to prosecution.

Unlawfully influencing the shareholders' meeting (Article 2636 of the Civil Code)

Persons who obtain a majority in the shareholders' meeting by simulation or fraud, in order to achieve an unfair profit for themselves or for others are punished with incarceration.

Market rigging (Article 2637 of the Civil Code)

This offence refers to the spreading false information or setting up simulated transactions or the use of other devices likely to significantly alter the price of financial instruments which are not listed and

[37] The crime of instigating bribery exists only if the offer or promise are made to, or the solicitation is formulated by directors, general managers, managers responsible for preparing the company's financial reports, statutory auditors or liquidators or other individuals vested with powers of management within a company or private entity. The same offence committed by/directed to employees who do not perform managerial functions does not constitute incitement.

[38] The reform of the crime of "*Private-to-private corruption*" and of "*Instigating private-to-private corruption*" was provided for in Legislative Decree 38/2017, which is in effect from 14 April 2017. Actions committed prior to that date were considered bribery among individuals only if the conduct actually constituted an action that was contrary to the duties and caused damage to the company the bribe-givers belonged to, and did not apply if the actions were against private entities that were not incorporated. The addition of private entities appears to be comprehensive and is not limited to associations and foundations with a legal personality.

for which no application for listing on a regulated market has been made, or likely to have a significant impact on public confidence in the financial stability of banks or banking groups.
For conduct that refers to issuers of listed instruments or instruments for which a request has been made for listing on a regulated market, the market abuse sanctions and connected administrative liability continue to apply.

Obstruction of the duties of the Public Supervisory Authorities (Article 2638 of the Civil Code)
This offence occurs when submitting mandatory communications to the public supervisory authorities, if untrue material facts are declared, albeit the subject of estimates, or facts that should have been reported are totally or partially concealed by fraudulent means, concerning the company's profit and loss, balance sheet or cash flow situation, for the specific purpose of obstructing the Supervisory Authority's activity.
This offence is also generated by any active or omissive conduct having the effect of hindering performance of the Supervisory Authorities' duties.
The penalty is increased if the offence involves a listed company or issuers whose financial instruments are widely distributed among the public.

False statements in prospectuses (Article 173-*bis* of Legislative Decree 58/1998)
Article 173-*bis* of Legislative Decree 58/98 punishes the conduct of any person who includes false information or conceals data or news in the prospectuses required for public offerings or for admission to trading on regulated markets, or in the documents required for public purchase or exchange offers.
For this conduct to constitute an offence, the person engaging in it must act with the intention of deceiving the recipients of the prospectuses, in order to obtain an unfair profit for himself or others. Moreover, the false or omitted information must be such as to lead their recipients into error.
At present, this does not constitute an offence in which corporate administrative liability is presumed[39].

7.4.2 Sensitive company activities

The sensitive activities identified by Model which involve the highest risks of corporate offences are the following:

- Management of relations with the Management Control Committee and the Independent Auditors;

[39] Article 25-*ter* of Legislative Decree 231/2001 even now makes no reference to Article 2623 of the Civil Code, which originally envisaged this offence. Law 262/2005 repealed the regulation and introduced the current offence of false statements in prospectuses pursuant to Article 173-*bis* of Legislative Decree 58/1998. As Article 25-*ter* was not subsequently amended, this seems to confirm that the offence of false statements in prospectuses does not constitute an offence in which corporate administrative liability is presumed. In this respect, the same principle indicated in the Court of Cassation judgement referred to in note 30 seems to apply.

- Management of periodic reporting;
- Preparation of the prospectuses
- Purchase, management and disposal of investments and other assets;
- Management of relations with Supervisory Authorities.

The next sections present, for the first four sensitive activities listed, the protocols setting out the principles of control and conduct applicable to these activities, which are supplemented by detailed company regulations governing them. With reference to private-to-private corruption in particular, this crime can have a potential far-reaching impact that affects all Bank activities, so reference is also made to the sensitive activities contemplated in the following protocols, as they contain principles for the effective prevention of this crime:

- Management of disputes and out-of-court settlements (paragraph 7.2.2.6);
- Management of the procedures for the procurement of goods and services and for the appointment of professional consultants (paragraph 7.2.2.8);
- Management of gifts, entertainment expenses, donations to charities and sponsorships (paragraph 7.2.2.9);
- Management of the staff selection and recruitment procedures (paragraph 7.2.2.10);
- Management of real-estate and cultural assets (paragraph 7.2.2.11).

Lastly, in relation to the activities indicated in the last point (Management of relations with Supervisory Authorities), reference should be made to the protocol in paragraph 7.2.2.7 which specifically aims to prevent not only various types of bribery but also the corporate offence contemplated in Article 2638 of the Civil Code.

Such protocols also apply to the monitoring of any activities performed by Group companies or outsourcers on the basis of special service agreements.

7.4.2.1. Management of relations with the Management Control Committee and the Independent Auditors

Introduction

This protocol applies to the members of the Board of Directors and to all the Bank's Bodies and Structures involved in the management of relations with the Management Control Committee and with the Independent Auditors at the time of checks and audits performed to fulfil legal requirements.

Pursuant to Legislative Decree 231/2001, the process in question might offer opportunities for commission of the offence of "Obstruction of controls", pursuant to Article 2625 of the Civil Code and of the offences referred to in Article 27 of Legislative Decree 39/2010 (with regard to the offence of false reporting or communications by the persons responsible for auditing, committed in conspiracy with bodies of the audited company) and in Article 29 of the same Decree (concerning the offence preventing or hindering the performance of statutory auditing activities), which are taken into account for the purposes of this protocol, notwithstanding the principle affirmed by the Court of Cassation mentioned, in paragraph 7.4.1 above - and are considered in any case for the purposes of this protocol.
Only as regards the management of relations with the Independent Auditors, there is also the risk of the commission of the offence of "*Private-to-private corruption*" and "*Instigating private-to-private corruption*", introduced by Law 190/2012 under corporate offences and described in paragraph 7.4.

The contents of this protocol are aimed at ensuring that the Bank complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in the management of the relations in question.

Process description

In the area of the monitoring activities vested in the Management Control Committee and in the Independent Auditors, management of relations with such bodies can be broken down as follows:

- submission of the required periodic reports;
- submission of corporate information and data and provision of documentation, based on specific requests.

The operating methods for managing the process are governed as part of internal regulations developed and updated by the competent Structures, which constitute an integral and substantial part of this protocol.

Control principles

The control system for monitoring the process must be based on the following elements:

- Authorisation levels defined within each operating step of the process. In particular, relations with the Management Control Committee, the Committees and the Independent Auditors shall be managed by the Head of the reference structure or by the persons specifically appointed by him.

- Segregation of duties is ensured between the different persons involved in the process of managing relations with the Management Control Committee, the Committees and the Independent Auditors, in order to guarantee that a maker and checker mechanism is in place in all phases of the process.

- Regular and ongoing participation of the Management Control Committee in Board of Directors meetings, to ensure that the Management Control Committee is effectively informed of the Bank's and the Group's operational choices.

- Prompt and timely fulfilment, by the relevant departments, of requests for specific documents made by the Management Control Committee and by the Committees – through the Governance function of the Internal committees and 231/2001 Surveillance Body - in the carrying out of its control and supervision activities.

- All requests for specific documents made by the Independent Auditors in performance of its audit, monitoring and administrative-accounting process assessment activities are promptly and fully met by the competent structures: each Structure shall collect and organise the information requested and deliver it, in accordance with the contractual obligations set out in the audit engagement contract. Records shall be maintained of all the documents provided in response to specific information requests formally made by the auditors.

- The structures concerned shall promptly and fully make available to the Independent Auditors the documentation they possess relating to the control activities and operational processes implemented, to enable the auditors to carry out their verifications.

- Process traceability including both the electronic and the paper trail:
  - all the monitoring and control activities carried out by the Management Control Committee and the Committees shall be systematically recorded and kept on file;
  - the supporting declarations for preparation of the Representation Letter, issued to the Independent Auditors, shall be checked and filed, and shall be signed by the Executive in charge of preparing the corporate accounting documents and by the Managing Director and C.E.O.;
  - in order to allow reconstruction of responsibilities and of the reasons for the choices made, the Structure from time to time concerned shall be responsible for filing and storing, also in

telematic or electronic format, all the documentation it has produced relating to performance of the requirements relating to management of relations with the Management Control Committee, the Committees and the Independent Auditors.

Rules of Conduct

The Banks Structures and Bodies howsoever involved in the management of relations with the Management Control Committee, the Committees and the Independent Auditors, have an obligation to act with the highest diligence, professionalism, transparency, collaboration and availability and to fully respect the institutional role of said governance bodies, promptly and accurately meeting all provisions and performing any requirements set out in this protocol, in compliance with the applicable provisions of law and with any relevant provisions of the Group's Code of Ethics and Internal Code of Conduct.

Specifically:

- periodic reports to the Management Control Committee, the Committees – through the Board governance Committees and the 231/2001 Surveillance Body and to the Independent Auditors must be submitted promptly, and any requests or demands received from them must be duly dealt with;
- The members of the Board of Directors and the employees who are for whatever reason involved in a request to submit documents or information made by the Management Control Committee or by any of its members or by the Committees – through the Secretariats of the Boards and General Affairs, – and of the Independent Auditors shall act with the highest correctness and transparency and shall in no way hinder monitoring and/or auditing activities;
- all data and documents shall be made available in a precise manner and using clear, objective and exhaustive language, so as to provide accurate, complete, faithful and truthful information;
- each Corporate structure shall be responsible for filing and keeping all the documents formally shown and/or delivered to the members of the Management Control Committee and of the Committees and to the Auditors, within the sphere of their activity, including all documents submitted in electronic format.

In any event, it is forbidden to initiate, cooperate/give rise to conduct that could be considered an offence in terms of Legislative Decree 231/2001, and, more specifically by mere way of example, to:

- delay without good reason or omit the presentation of documents/communication of requested data;
- present incomplete documents and data and/or communicate false or altered data;
- adopt deceitful conduct which might lead the Management Control Committee, the Committees and the Independent Auditors into error in the technical-economic assessment of the documents submitted;
- promise or give sums of money or other benefits to members of the Independent Auditors, with the purpose of promoting or furthering the Bank's interests..

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.4.2.2. Management of periodic reporting

Introduction

This protocol applies to all the Bank Structures involved in the preparation of the documents that contain communications to shareholders and/or to the market concerning the Bank's profit and loss, balance sheet and financial situation.
Pursuant to Legislative Decree 231/2001, the process to prepare the documents in question could pose a risk of committing the offence of "*false corporate reporting*", as regulated in Articles 2621 and 2622 of the Civil Code, as well as tax crimes, indicated in paragraph 7.12 (Sensitive area concerning tax crimes). Furthermore, the company rules and the controls of completeness and truthfulness envisaged in this protocol are also arranged with a view to providing more extensive preventive action against offences that could arise from incorrect management of financial resources, such as "*Corruption against the Public Administration*" in its various forms, "*Illegal inducement*" "*Private-to-private corruption*" and "I*nstigating private-to-private corruption*" as well as the offences of "*Money laundering*" and "*Self-laundering*".

The process of preparing the documents in question is governed by guidelines contained in the Company's Regulation approved by the Management Body, with the control body's favourable opinion, in response to the indications set out in Law 262/2005 and in particular in Article 154-*bis* of the Finance Consolidation Act, which introduced the role of "Manager responsible for preparing a company's financial reports" assigning the incumbent specific responsibilities aimed at ensuring a truthful and fair representation of Group's profit and loss, balance sheet and financial situation.

The "Guidelines for administrative and financial governance" set out the reference principles and the roles and responsibilities assigned to the Bank's structures in respect of the process covered by this Protocol, of which they form an integral part. These Guidelines provide, in particular, that the sensitive procedures relating to financial disclosures shall be formalised and verified, in order to assess their compliance with the requirements of Article 154-*bis* of the Finance Consolidation Act; therefore, the procedures set out in the regulation constitute the detailed operational rules of this protocol.

Besides the above Guidelines, specific governance documents and rules, updated from time to time, are used for the governance and process of preparing documents containing communications to the shareholders and/or to the market concerning the Bank's financial position and performance and cash flows, including:

- the "Guidelines for the governance of financial disclosure to the market (Financial Statements and Pillar III);
- "Guidelines for evaluating financial statement items";
- "Group accounting rules";
- regulations on Fair Value;
- "Rules on preparing disclosure to the public Pillar III".

The definitions given in this protocol are aimed at ensuring the Bank's compliance with applicable regulations and principles of transparency, correctness, objectivity and traceability in carrying out the activities concerned.

Process description

As regards processes that are sensitive for the purposes of financial disclosure, activities that are strictly functional for producing financial statements, the consolidated financial statements and interim reports, are particularly significant. Such activities fall under the following corporate processes:

- Management of the accounts and of supervisory communications;
- Management of the individual financial statements and consolidated financial statements.

The operating methods for managing the process are governed as part of internal regulations developed and updated by the competent Structures, which constitute an integral and substantial part of this protocol.

Control principles

The documents containing communications to the shareholders and/or to the market concerning the Bank's profit and loss, balance sheet and financial situation must be prepared in accordance with the specific corporate procedures, practices and systems in force which:

- identify in a clear and exhaustive manner the functions concerned and the data and information they must provide;
- identify criteria for recognising corporate events in the accounts, including the recognition of individual items;
- define the deadlines, the matters to be communicated and disclosed, organisation of the related flows of information and any request for the issue of specific declarations;

- provide for the transmission of data and information to the Structure responsible for collecting them through a system that ensures the traceability of the individual transactions and identification of the persons that enter the data into the system;
- establish criteria and procedures for processing the data of the consolidated financial statements and for the forwarding of such data by the companies belonging to the scope of consolidation.

The control system for monitoring the process described above must be based on the following elements:

- Specifically defined roles and responsibilities:
  - each Structure is responsible for the processes that contribute to generating accounting items and/or for the valuation activities assigned to it, and for any comments to the financial statements falling within its sphere of competence;
  - the power and delegation system establishes the degree of operational autonomy in respect of the activity in question, in particular with regard to the recognition of losses;
  - Different user profiles are defined for accessing IT procedures, matching specific authorisation levels based on assigned functions;
  - the adequacy of the sensitive processes relating to accounting and financial reporting and of the related controls shall be monitored by a specific structure reporting to the Manager responsible for preparing the company's financial reports, and by the Internal Auditing function in performance of its activity.

- Segregation of functions
  - The process of preparing the documents containing communications to shareholders and/or to the market concerning the Banks' profit and loss, balance sheet and financial situation involves several Structures, which operate in the different phases of the process in accordance with the instructions provided in the "Guidelines for administrative and financial governance".

- Control activities
  - The activities of preparing the documents containing communications to the shareholders and/or to the market concerning the Bank's profit and loss, balance sheet and financial situation shall be carefully and thoroughly checked for completeness and accuracy, using both automated and manual systems. The main controls performed by the individual Structures are as follows:
    - periodic checks of the balances of the accounting items in general, in order to ensure the clearance of the accounts;
    - verification, at pre-established intervals, of all balances of work in progress, temporary accounts and similar accounts, to ensure that the Units concerned which have fed the accounts make the necessary entries under the appropriate headings;
    - existence of maker and checker controls ensuring that the person executing the transaction is different from the person who authorised it after checking its appropriateness;

  - for all transactions recorded in the accounts a duly validated first accounting entry is made, and the associated supporting documents are provided;
  - any changes are analysed by comparing the accounting data for the current period with that recorded in the previous periods;
  - a control on the merit is carried out when opening new accounts and updating the account plan;
  - harmonisation of the final version of the financial statements with the accounting data.
- Verification of the adequacy of the sensitive processes for accounting and financial reporting purposes and of the effective application of the associated controls comprising the following phases:
  - verifying the design of the controls;
  - testing actual application of the controls;
  - identifying problem areas and defining corrective action plans;
  - monitoring the progress and effectiveness of the mitigation actions undertaken.

- Process traceability including both the electronic and the paper trail:
  - the decision-making process for preparing the documents containing communications to the shareholders and/or to the market concerning the Bank's profit and loss, balance sheet and financial situation is guaranteed by the complete traceability of each accounting operation, both via the IT system and on paper support;
  - all the adjusting entries made by the individual Structures with regards to the accounts under their competence or by the Structure responsible for the management of the Financial Statements shall be supported by appropriate documentation indicating the criteria adopted and providing an analytical view of the development of calculations;
  - all the documentation concerning the periodic controls carried out shall be kept on file by each Structure involved in respect of the accounting items under its competence;
  - all the documents supporting preparation of the financial statements shall be kept on file by the Structure responsible for management of the Financial Statements and/or by the structures involved in the financial reporting process.

Rules of Conduct

The Bank's structures howsoever involved in bookkeeping activities and in the subsequent preparation/filing of corporate reports on the Bank's profit and loss and asset situation (annual financial statements, consolidated financial statements, reports on operations, quarterly and half-yearly reports, etc.) are required to comply with the procedures set out in this document, with the applicable provisions of law, with the "Guidelines for administrative and financial governance" and with the procedures governing the activity in question; all such rules are based on principles of transparency, accuracy and completeness in financial reporting, for the purpose of producing fair and timely views of the profit and loss, asset and financial situation, also in accordance and for the

purpose of Articles 2621 and 2622 of the Civil Code. In particular, Bank Structures have an obligation to:

- represent operations correctly, completely and promptly in the company accounts and data, in order to guarantee a true and fair view of the financial position, performance and cash flows of the Bank;
- adopt at all times a correct, transparent and cooperative approach, in compliance with the rules of law and with internal corporate procedures, in all the activities for the preparation of the financial statements and other corporate disclosure, in order to provide shareholders and third parties with a true and fair view of the Bank's financial position, performance and cash flows.

In any event, it is forbidden to initiate, cooperate/give rise to conduct that could be considered an offence in terms of Legislative Decree 231/2001, and, more specifically by mere way of example, to:

- recognise or transmit for processing and recognition in financial statements, reports and prospectuses or in other corporate communications, false, incomplete or howsoever inaccurate data on Bank’s and Group’s profit and loss, balance sheet and financial situation;
- omit data and information imposed by the law on the Bank’s and the Group's profit and loss, balance sheet and financial situation.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.4.2.3. Preparation of the prospectuses

Introduction

This protocol applies to all the Bank Structures involved in preparation of the Prospectuses[40] required for public offerings or for admission to trading on regulated markets, or in the documents to be published when public purchase or exchange offers are launched. The related process could present opportunities for commission of the offence of "False statements in prospectuses ", set out in Article 173-*bis* of the Finance Consolidation Act, and implies clear connections with the procedures in place for the prevention of market abuse conduct; although there are serious doubts as to whether the offence of "False statements in prospectuses" might involve the administrative liability of Entities, as stated in the section illustrating the types of offences (paragraph 7.4.1), it is nevertheless advisable to put in place specific control and conduct principles to monitor such process. The Prospectus contains the information "*that, depending on the characteristics of the financial products and the Issuers, is necessary for investors to make an informed assessment of the Issuer's assets and liabilities, profits and losses, financial position and prospects and of the financial products and related rights*". In the event of public offers to buy or exchange financial instruments, the Document shall contain "*the information that is necessary for investors to make an informed assessment of the offer*".

The definitions given in this protocol are aimed at ensuring the Bank's compliance with applicable regulations and principles of transparency, correctness, objectivity and traceability in carrying out the activities concerned.

Process description

In compliance with current legislation, the prospectus preparation process comprises the following phases:

- collecting and analysing the information necessary to prepare the prospectuses;
- signing declarations of responsibility on the content of prospectuses;
- certification by the Financial Reporting Manager, pursuant to Article 154-*bis* of the TUF (only for own issues);
- forwarding of the prospectuses and management of relations with the competent Authorities.

The operating methods for managing the process are governed as part of internal regulations developed and updated by the competent Structures, which constitute an integral and substantial part of this protocol.

[40] Pursuant to Legislative Decree 58 of 24/2/1998 as subsequently amended (inter alia by Law 262 of 28/12/2005) and pursuant to Directive 2003/71/EC of 4/11/2003 as transposed by Commission Regulation (EC) No 809/2004 of 29 April 2004. The Prospectuses referred to are both those relating to issues in the domestic market and those relating to the issue of securities in the international markets.

Control principles

The system of controls for monitoring the process described is based on the following factors:

- Expressly defined authorisation levels:
  - the Bank, taking into account the provisions of Article 154-*bis*, paragraph 3 of the Finance Consolidation Act, shall identify the Structures responsible for preparing and drafting the various Sections of the Prospectuses, identifying, within their respective missions or through formal delegation, the Structures responsible for preparing, signing and forwarding the prospectuses to the Authorities (only for own issues);
  - the relations with the competent Authorities shall be held by duly empowered persons, in compliance with the rules of conduct laid down in the protocol "*Management of relations with the Supervisory Authorities*";
  - securities issuance or listing transactions must be approved by the statutory governance bodies of the Bank.

- Segregation of duties:
  - the Prospectus preparation process sees the participation of several Bank Structures and, if required, qualified support from external legal practices, which are responsible, each within the scope of its competences, for organising the information and drafting the documents necessary for preparing the Prospectuses.

- Control activity by each competent Structure and in particular:
  - controls on the completeness, correctness and accuracy of the information provided in the documents falling under each Structure's competence, which must be supported by maker and checker mechanisms;
  - legal controls on compliance with the reference legislation.

- Process traceability including both the electronic and the paper trail:
  - each relevant phase of the Prospectus drafting process must be recorded in specific written documents;
  - in order to allow reconstruction of responsibilities and of the reasons for the choices made, the Structure from time to time concerned shall be responsible for filing and storing, also in telematic or electronic format, all the documentation it produced relating to performance of the requirements associated with preparation of the Prospectuses.

Rules of Conduct

The Bank's Structures howsoever involved in preparation of the Prospectuses shall comply with the procedures set out in this protocol, with the applicable provisions of law, the internal rules and any provisions of the Group's Code of Ethics and Internal Code of Conduct.

In particular all Bank Structures involved have an obligation to:

- maintain at all times correct, transparent and co-operative conduct in order to ensure protection of investors' savings;
- employ the maximum attention and accuracy in each activity aimed at collecting, processing and presenting data and information on the financial products necessary for investors to make an informed assessment on the Bank's and the Group's profit and loss, balance sheet and financial situation;
- if third parties are to be involved in preparation of the Prospectuses, the contracts entered into with such persons shall contain a specific declaration that they know the provisions of Legislative Decree 231/2001 and undertake to comply with them.

For the correct management of the information underlying issue of the Prospectuses, reference is also made to the rules of conduct contained in the protocol reproduced in paragraph 7.8.2.1, concerning the "*management and disclosure of information and external communication for the purposes of preventing criminal and administrative offences in the area of market abuse*".

In any event, it is forbidden to initiate, cooperate/give rise to conduct that could be considered an offence in terms of Legislative Decree 231/2001, and, more specifically by mere way of example, to:

- prepare Prospectuses or offer documents that are incomplete and/or contain false or altered data.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.4.2.4. Purchase, management and disposal of investments and other assets

Introduction

This protocol applies to all Bank structures involved in the purchase, management and disposal of investments – direct or indirect, qualified or unqualified – in the share capital of other companies, including investments in special purpose acquisition companies (SPAC), in which the Bank is Co-Promoter, or in other forms of investment/divestment similar to the undertaking/disposal of an equity investment (for example, subscription of convertible bonds or equity instruments) and other assets (for example, non-performing loans, business units, assets and legal relationships identified in blocks).

Pursuant to Legislative Decree 231/2001, the related process could present opportunities for the commission of “Private-to-private corruption” and “Instigating private-to-private corruption” and “Failure to disclose conflict of interest”.

The definitions given in this protocol are aimed at ensuring the Bank's compliance with applicable regulations and principles of transparency, correctness, objectivity and traceability in carrying out the activities concerned.

Process description

The process can be broken down as follows:

- examination of the feasibility of the transaction and/or identification of investment and/or funding opportunities;
- management of pre-contractual relationships and performance of activities preliminary to the signing of the contract (regulatory compliance verification, due diligence, etc.);
- finalisation of the contract;
- management of the obligations related to the purchases, management and disposal of investments (including the assignment of officers to the investee) and other assets.

With specific reference to the activities carried out by the Bank in relation to the promotion of SPAC, the process comprises several phases such as the identification of new opportunities for SPAC and new partners, the establishment of pre - Initial Public Offering (IPO) vehicle, the IPO, scouting and business combinations or liquidation.

The operating methods for managing the process are governed as part of internal regulations developed and updated by the competent Structures, which constitute an integral and substantial part of this protocol.

Control principles

The system of controls for monitoring the process described is based on the following factors:

- Expressly defined authorisation levels. Specifically:
  - persons exercising authorisation and/or negotiating powers at each phase of the process are identified and authorised on the basis of their specific role assigned by the organisational code or by the Head of the reference Structure by means of internal delegation, kept on file by the same Structure;
  - deeds and documents binding to the Bank must be signed by persons with the necessary powers to do so;
  - the delegated powers system establishes the right of independent management in relation to investments; internal regulations illustrate the aforementioned authorisation mechanisms, providing an indication of the corporate officers holding the necessary powers.

  With specific reference to the activities carried out by the Bank in relation to the promotion of SPAC, the establishment of the SPAC and the subsequent business combination, said are authorized by the optional bodies subject to the binding opinion of the specific Session required by internal regulations.

- Segregation of duties among persons involved in the process in order to guarantee maker and checker mechanisms between the phases of the process.

  With specific reference to the activities carried out by the Bank in relation to the promotion of SPAC, the Bank cannot take on the role of NoMad and Specialist and must always use at least one Joint Global Coordinator, in addition to the Bank itself. Scouting, i.e. searching for operational target companies potentially subject to business combinations with the SPAC promoted by the Bank, must be carried out by third parties other than the Bank itself.

- Control activities:
  - verification of the preliminary assessment performed in accordance with the internal regulation, by executing specific due diligence activities as required (e.g. economic/financial, accounting, legal, tax-related, etc.) in relation to the target company and its counterparty particularly as regards the provisions of the Anti-Corruption Guidelines;

- verification that the resolution contains the transaction pricing criteria in accordance with market practices;
- verification of compliance with legal and regulatory obligations (e.g. regarding anti-money laundering);
- verification of the keeping and updating of records of existing investments;
- verification of the periodic assessment process for existing investments as part of the preparation of Company's separate and consolidated financial statements.

With specific reference to the activities carried out by the Bank in relation to the promotion of SPAC, the following are envisaged:

- when setting up and placing the SPAC, checks on the overall investment in institutional SPACs and on the amount per single investment;
- in the business combination phase, checks on compliance with the ban on scouting target companies, on compliance with due diligence activities and verification of requirements relating to credit and/or equity investment relationships that may exist between the Intesa Sanpaolo Group and the target company (together with the group headed by the target), both at this phase and after the completion of the transaction.

- Process traceability including both the electronic and the paper trail:
  - each significant phase of the activity regulated by this protocol must be recorded in a specific written document;
  - every agreement/convention/contract/other formality instrumental to the purchase, management and disposal of investments and other assets is formalised in a document duly signed by persons with suitable powers to do so on the basis of the existing delegated powers system;
  - in order to allow reconstruction of the responsibilities and motivations underlying the preliminary assessment conducted for making the investment and the decisions made during its management and disposal of investments and other assets, each Structure is responsible for archiving and storing the documentation it produces, also digitally or electronically, in relation to this protocol.

  With specific reference to the activities carried out by the Bank in relation to the promotion of SPAC, periodic reporting of operations carried out is envisaged, also in order to allow the Group Risk and Sustainability Committee to monitor project aspects.

- Bonus or incentive systems: bonus and incentive systems must be able to guarantee compliance with legal provisions, the principles of this protocol and the provisions of the Code of Ethics, also envisaging suitable corrective mechanisms for any conduct deviating from the norm.

Rules of Conduct

The Bank's Structures involved in any manner in the purchase, management and disposal of investments and other assets process are obliged to abide by the methods illustrated in this protocol, existing legal provisions on such matters, internal regulations and any provisions of the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines. Specifically:

- persons exercising authorisation and/or negotiating powers at the pre-contractual, contractual and management phases of investment relationships must be identified and authorised on the basis of their specific role assigned by the organisational code or by the Head of the reference Structure by means of an internal delegation, kept on file by the same Structure;
- documentation relating to contracts for the purchase, management and disposal of investments and other assets must comply with current general and special regulations for the reference sector, also by seeking advice from the competent company departments and/or external professionals;
- employees must not accept any demand for sums of money or other benefits made directly or of which he/she may become aware, formulated by senior officers or their staff in companies that are counterparties or in relationships with the Bank, with the aim of performing or failing to perform an act contrary to the obligations of their specific duties or obligations of loyalty, and must immediately report any such cases to their direct superior; the superior shall in turn forward the report received to Internal Auditing for appropriate assessment and the completion of any formalities to the Surveillance Body in accordance with the provisions in paragraph 4.1.;
- if the involvement of third parties is envisaged in the signing and/or management of contracts relating to the purchase, management or disposal of investments and other assets, the agreements with such parties must contain a special declaration of awareness of the regulations contained in Legislative Decree 231/2001 and the provisions of the laws against corruption and a commitment to comply with such regulations;
- the payment of fees or compensation to external collaborators or consultants involved is subject to permission given in advance by the organisational unit responsible for assessing service quality and the resulting fairness of the fee demanded; in any case, no remuneration shall be payable to employees or external consultants where not fully justifiable by current or future activities;
- employees designated by the Bank to act as members of the Board of Directors of an investee company are obliged to inform the latter – in the formats and terms envisaged in Article 2391 of the Civil Code − of any interest they may have, on behalf of the Bank, on their own behalf or for third parties, in a given transaction of the company in question, abstaining from executing the transaction if acting as managing director.

In any case, it is forbidden to initiate/collaborate in/give rise to conduct that could be construed as an offence pursuant to Legislative Decree 231/2001, and more specifically, purely by way of example, to:

- make false or altered information;

- promise or pay/offer undue sums of money, gifts of services free of charge (outside the accepted practices of courtesy gifts of little value) and grant advantages or other benefits of any kind – directly or indirectly, for oneself or for others – to directors, general managers, managers in charge of preparing the company's financial statements, statutory auditors or liquidators of companies, or persons under their management or supervision, in order to obtain from such persons the performance or failure to perform an act contrary to their official duties or obligations of loyalty to further or favour the interests of the Bank. Examples of such improper advantages include, without limitation, the promise to hire family members and relatives, disbursement of credit under terms not compliant with the principles of sound and prudent management envisaged in company regulations, all banking or financial transactions which generate a loss for the Bank and a profit for the aforementioned persons (e.g. unjustified cancellation of a debt position and/or application of discounts or conditions not in line with market parameters);
- award appointments to external consultants without following substantiated and objective criteria addressing professionalism and expertise, competitiveness, price, integrity and the ability to provide effective assistance. In particular, the rules for the selection of consultants shall refer to the criteria of clarity and availability of documentary evidence laid down in the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.5 Sensitive area concerning crimes with the purpose of terrorism or subversion of the democratic order, organised crime, transnational crimes and crimes against the person, as well as sports fraud and illegal betting or gaming

7.5.1 Offences

Introduction

Through a series of legislative acts, the framework of the administrative liability of Entities has been expanded to include various categories of offences, with the common aims of combating types of crime which raise particular concern at international level, specifically crimes of political terrorism, organised crime, including international organised crime, and crimes which violate fundamental human rights.

The banking industry - and our Bank's policy in line with it – has always paid particular attention and has always been strongly committed to cooperation in the prevention of criminal phenomena in the financial market and to the fight against terrorism; the Bank's commitment stems also from the aim of protecting sound and prudent management, transparency and correct behaviour and the proper functioning of the overall system. Furthermore, banking activity is especially exposed to the risk of making available to customers operating in sectors banned by law (for example the manufacture and sale of anti-personnel mines and cluster bombs) and/or belonging to or close to criminal organisations services, financial resources or other economic means which may be instrumental to the pursuit of illegal activities.

The types of crimes in question are summarised below.

* * *

Section I - Crimes for the purposes of terrorism or subversion of the democratic order

Under Article 25-*quater* of the Decree an entity shall be punishable, where there are appropriate grounds, in the event that the crimes for the purpose of terrorism or subversion of the democratic order provided for by the Criminal Code, the special laws and by the International Convention for the Suppression of the Financing of Terrorism signed in New York on 9.12.1999, are committed in the interest of or for the benefit of the entity.

This provision sets out no fixed or mandatory list of crimes, but refers to any criminal offence whose author specifically pursues aims of terrorism or subversion of the democratic order[41].

[41] Article 270-*sexies* considers as having terrorist purposes those conducts which can cause considerable damage to a Country or international organization and are committed in order to intimidate the population or force public authorities or an international organization to perform or restrain from performing any deed or destabilize or destroy fundamental political, constitutional, economic and social structures, as well as the other conducts defined as terrorist or committed for the purpose of terrorism by conventions or other international law provisions which are binding for Italy. According to case law (Criminal Court of Cassation, judgement 39504/2008) the expression "subversion of the democratic order" cannot be limited to the concept of violent political action alone, but should rather refer to the Constitutional order, and therefore to any means of political struggle aimed at subverting the democratic and constitutional order or at departing from the fundamental principles governing them.

The main types of such offences which might apply are listed below.

A) Crimes for the purpose of terrorism and subversion of the democratic order provided for by the Criminal Code or by special criminal laws.

These are political crimes, i.e. crimes against the State's domestic and international personality, against citizens' political rights and against foreign countries, their heads and their representatives.

The types of offences presenting a higher risk of occurrence during performance of banking activity are those of **"Financing terrorist activities"** (Article 270-*quinquies* 1 of the Criminal Code)**, the "Embezzlement of confiscated assets or monies"** (Article 270-*quinquies* 2 of the Criminal Code)**, "Participation in financing the enemy"** (Article 249 of the Criminal Code)**, "Kidnapping for purposes of terrorism or for subversion of the democratic order"** (Article 289-*bis* of the Criminal Code) and the offence set out in Article 270-*bis* of the Criminal Code**,** concerning **"Associations for the purpose of terrorism, including international terrorism, or of subversion of the democratic order".** In particular, this last offence also concerns any type of financing of associations which intend carrying out violent acts for the purpose of terrorism or subversion of the democratic order.

Attention should also be focused on financial offences, in particular money laundering and use of money, goods or other assets of unlawful origin, naturally if such offences are instrumental to the pursuit of the aims of terrorism or subversion of the democratic order.

In addition to the provisions of the Criminal Code, other relevant offences are set out in special laws covering a broad range of criminal activities (e.g. concerning weapons, drug trafficking, environmental protection, etc.) and in laws adopted in the 1970s and 1980s to combat terrorism (e.g. laws on the security of air and sea travel, etc.).

B) Crimes for the purpose of terrorism addressed by the 1999 New York Convention.

The reference to this Convention by Article 25-*quater*, paragraph 4, of the Decree clearly aims at avoiding any gaps as its intent is to further international cooperation for the suppression of the fund collecting and financing in any form to be used for terrorist activities in general or in sectors and concerning methods that entail a greater risk, which are the object of international treaties (air and maritime transport, diplomatic representations, nuclear, etc.).

* * *

Section II - Organised crime offences

Article 24-*ter* of the Decree, inserted by Law 94/2009, firstly sets out a group of offences relating to the various forms of criminal organisations, namely:

- Generic Criminal association (Article 416 of the Criminal Code, paragraphs 1 - 5);
- Mafia-type criminal association – including foreign organised crime association – and vote exchange in elections (Articles 416-*bis* and 416-*ter*);

- Criminal association for the purpose of committing the crimes relating to slavery, human trafficking and the smuggling of migrants (Article 416 of the Criminal Code, paragraphs 6 and 7);
- Association for the purpose of illicit trafficking in narcotic or psychotropic drugs (Article 74 of Presidential Decree 309/1990).

With reference to the types of criminal association listed above, it should be noted that the offence consists in promoting, establishing and participating in a criminal association consisting of three or more persons, and is therefore punishable per se regardless of whether or not the crimes pursued by the association are actually committed (any such crimes being punished separately). Consequently, the intentional participation of a representative or employee of the entity in a criminal association might of itself give rise to the entity's administrative liability, provided, of course, that participation in or support for such criminal association is also in the entity's interest or gives an advantage to it. Moreover, the association must involve at least some form of stable organisation and a common plan to carry out an indefinite series of crimes. In other words, an occasional agreement for the commission of one or more specific crimes does not constitute the offence of criminal association. Under case law moreover, the offence of aiding and abetting a criminal association is committed by a person who, while not being a member of such association, contributes in a significant manner, albeit occasionally, to its existence or to the pursuit of its objectives.

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

This provision also applies to the 'camorra' and other criminal organisations, howsoever named, including foreign crime syndicates, possessing the above-mentioned mafia-type characteristics. The crime of vote exchange in elections is committed by a person who proposes or accepts the promise to procure votes with the use of mafia methods against the payment or the promise of money or other benefits.

Lastly, the other two types of criminal association (Article 416, paragraphs 6 and 7 of the Criminal Code and Article 74 of Presidential Decree 309/1990) are characterised by their being set up to pursue specific crimes, namely: respectively, the offences relating to reducing into slavery, human trafficking and the smuggling of immigrants, organ trafficking, sexual crimes against minors and the offences of unlawful production, trafficking or possession of drugs of abuse or psychotropic substances. Some of these specific purpose-oriented offences are in themselves autonomous predicate offences giving rise to the Entity's liability, as discussed in greater detail below, in the section on crimes against the person and transnational crimes.

Article 24-*ter* also includes the generic category of any type of crime committed using mafia methods or in order to further the activity of a mafia-type association; in this case too, the Entity can be held liable only where the crime was aimed at pursuing its interest or giving it an advantage.
The first circumstance occurs when the perpetrator, while not belonging to the criminal organisation or aiding and abetting it, engages in specific intimidating conduct, for example making threats by exploiting the "reputation" of criminal organisations operating in a specific territory. The case of an offence furthering the activity of a mafia-type association occurs when the perpetrator acts with this specific aim in mind and his conduct is likely to achieve the intended result, for example where a money laundering offence is committed in the awareness of the fact that the operation concerns a mafia-type organisation.
Lastly, Article 24-*ter* also refers the following offences, which are usually, albeit not necessarily, committed by criminal organisations.

Kidnapping for ransom (Article 630 of the Criminal Code).
The offence consists of kidnapping a person in order to secure for oneself or others unlawful gain in exchange for release of the kidnapped person. The benefit may also consist in a non-financial advantage. In particular cases, this offence might also apply to persons who did not take part in the kidnapping but took steps to ensure that the kidnappers would obtain the ransom, by contributing to the lengthening of the negotiations and consequently of the kidnapped person's deprivation of liberty, or by helping the kidnappers obtain the ransom. Moreover, the offence of money laundering could apply to any persons playing a role in the transfer, circulation or use of sums of money or other goods, knowing that such sums were obtained through the offence in question.

Crimes relating to weapons and explosives (Article 407 paragraph 2, point a), no. 5 of the code of criminal procedure).
These are offences laid down by the special laws on the subject (in particular Law 110/1975 and Law 895/1967), which punish the unlawful manufacturing, introduction into the country, sale, supply, possession and unauthorised carrying of explosives, weapons of war and common firearms, with the exception of firearms used on shooting ranges, and of gas or compressed-air firearms. In this case too, similarly to the previous offence, any type of collusion by the bank operators with the perpetrators of such offences, or the performance of activities such as, for instance, the granting of financing, with the awareness of favouring such offences, even merely indirectly, could give rise to the offence of aiding and abetting such crimes, or to other offences, e.g. money laundering.
For information, it should be noted that Law 220/2021 "Measures to combat the financing of companies manufacturing anti-personnel mines, cluster bombs and submunitions", has specifically banned the funding of companies based in Italy or abroad that, directly or through subsidiaries or associates, carry out activities for the construction, production, development, assembly, repair,

retention, use, deployment, warehousing, storage, possession, promotion, sale, distribution import, export, transfer or transport of anti-personnel mines, cluster bombs and submunitions, of any type or composition, or parts of said.

The Law establishes in particular that qualified intermediaries[42] that fail to observe this ban will be punished with an administrative fine from 150,000 euros to 1,500,000 euros, for the cases contemplated in Article 5 of Legislative Decree 231 of 8 June 2001 (for violations committed in their interest or to their benefit)[43].

* * *

Section III - Transnational offences

The liability of Entities for this category of offence is laid down in Law 146/2006, in order to enhance the effectiveness of the fight against transnational organised crime.

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

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

We describe below the criminal offences which may give rise to the Entity's liability where the twofold conditions of the entity's interest or advantage and of the translational nature of the crime (of which the offender must have been aware) are met.

Criminal associations under Articles 416 and 416-*bis* of the Criminal Code criminal associations for the smuggling of foreign tobacco products (Article 291-q*uater* of Presidential Decree 43/1973)[44] or for trafficking in drugs of abuse (Article 74 of Presidential Decree 309/1990)

[42] Italian investment companies (SIM), Italian banks, Italian asset management companies (SGR), open-end investment companies (SICAV), financial intermediaries registered with the list as indicated in Article 106 of the consolidated act as per Legislative Decree no. 385 of 1 September 1993, including credit guarantee consortia, banks of EU Member States, investment firms of EU Member States, non-EU banks, stockbrokers registered with the single register kept by the Ministry of Economy and Finance, as well as banking foundations and pension funds.

[43] In keeping with the values and principles in the Code of Ethics, Intesa Sanpaolo S.p.A. prohibits any type of banking and/or financing activity connected with the production and/or sale of weapons that are controversial and/or banned by international treaties, such as: (i) nuclear, biological and chemical weapons; (ii) cluster and fragmentation bombs; (iii) weapons containing depleted uranium; (iv) anti-personnel land mines.

[44] The cases in Article 291 quater of Presidential Decree 43/73 are referred to in Article 25 *sexiesdecies* of Legislative Decree 231/2001.

The basic characteristics of the conduct constituting criminal association are described above in the paragraphs on criminal association offences. We believe that, where such offences are of a transnational nature, the only penalties that might be applicable to the entity are those set out in Law 146/2006 but not those set out in Article 24-*ter* of the Decree.

Offences relating to the smuggling of migrants (Article 12, paragraphs 3, 3-*bis*, 3-*ter* and 5 of Legislative Decree 286/1998)[45]

Article 12 punishes the illegal transport of foreigners into the territory of the State, as well as the promotion, coordination, organisation or financing of such transport, and other acts aimed at facilitating the illegal entry of foreigners into the territory of Italy or of another country different from their country of origin or habitual residence. However, at least one of the five conditions listed in the Article must be met for this offence to take place[46].

The punishment is increased where at least two of the above-mentioned conditions are met at the same time, or where the acts were committed for specific aims such as: the recruitment of persons to be destined for prostitution; the exploitation of minors, or, in general, in order to obtain a profit, even indirectly.

Lastly, paragraph 5 punishes complicity in the permanence of a foreigner in order to obtain an unfair gain from such foreigner's illegal status. Unfair gain is deemed to occur when the balance of services is altered as a consequence of the fact that the offender is aware of the foreigner's illegal status and exploits to his advantage.

Inducement not to make or to make false statements to judicial authorities (Article 377-*bis* of the Criminal Code)

This offence occurs when anyone uses violence or threats, or offers or promises money or other benefit to induce not to make statements, or to make false statements any person who is called before the judicial authorities to make statements in connection with criminal proceedings if such person has the right to remain silent.

This offence can entail the Entity's liability even where the transnational element is absent, since it is referred to not only by Law 146/2006, but also by Article 25-*decies* of the Decree.

Aiding a fugitive (Article 378 of the Criminal Code)

This offence consists of helping the author of a crime punishable by life imprisonment or a prison sentence – after the deed, and without having aided and abetted its commission – to avoid

[45] Offences relating to the smuggling of migrants, despite not having transnational characteristics, give rise to liability pursuant to Legislative Decree 231/2001 as from 19.11.2017, the date when article 25- duodecies , paragraph 1- bis , of the Decree, introduced by Law No. 161/2017, came into effect.

[46] In brief: a) the act concerns the illegal entry or residence in Italy of five or more persons; b) the smuggled persons' life or safety were endangered; c) the smuggled persons were subjected to inhumane or degrading treatment; d) the act was committed by three or more persons acting in association with one another or utilising international transport services or documents that are forged or altered or were in any way illegally obtained; e) the act was committed by persons possessing arms or explosives.

investigation by the authorities or arrest. The offence occurs even if the person so assisted cannot be charged with the crime or is found not to have committed it. The penalty is increased when the crime in question is that of participation in a mafia-type association.

It should be noted that according to prevailing case law, this offence is also committed by those who give false replies on being questioned by the Judicial authorities.

* * *

Section IV - Crimes against the person

Article 25-*quinquies* of the Decree lists certain offences against individuals set out in the Criminal Code in order to forcefully combat new forms of slavery such as prostitution, human trafficking, the exploitation of children and forced begging, which are all activities strongly associated with the spread of organised crime and new criminal organisations.

In particular, the following types of crimes are identified: **"Enslaving or keeping persons enslaved or in servitude" (Article 600 of the Criminal Code), "Child prostitution" (Article 600-*bis* of the Criminal Code), "Child pornography" (Article 600-*ter* of the Criminal Code), "Possession of or access to child pornography material" (Article 600-*quater* of the Criminal Code), "Virtual pornography" (Article 600 – *quater*.1 of the Criminal Code) "Tourism initiatives aimed at exploiting child prostitution" (Article 600-*quinquies* of the Criminal Code), "Solicitation of minors (Article 609-*undecies* of the Criminal Code), "Human trafficking" (Article 601 of the Criminal Code), "Purchasing and selling slaves" (Article 602 of the Criminal Code).**

Lastly, it should be noted that Article 25 *quater* paragraph 1 provides for the administrative liability of the Entity for the crime against the person referred to in Article 583-*bis* of the Criminal Code. (Female genital mutilation practices).

The risk of the entity being liable for the above-mentioned crimes can only be deemed to be significant in the event that a Bank representative or employee acts in conspiracy with the material author of the offence. The type of conspiracy where risk is greatest is linked to financing by the Bank of organisations or of persons that commit any of the above-mentioned offences.

The following offences can also be included in this section:

- ***"Employment of foreign nationals with irregular permits of stay"*** (Article 22, paragraph 12-*bis*, Legislative *Decree* 286/1998 – Consolidated Law on Immigration, which is mentioned in art, 25-duodecies of the Decree[47]), which punishes employers that hire or make use of non-EU employees without a regular residence permit, or with a permit that has expired without requesting renewal, or has been revoked or cancelled. Corporate liability for this offence, which is connected to the exploitation of illegal workers, is only envisaged in certain aggravated circumstances[48];

[47] Article 25-*duodecies* was inserted into Legislative Decree 231/2001 by Article 2 of Legislative Decree 109/2012, effective from 9.8.2012.
[48] One of the following circumstances has to exist: a) employment of more than three workers without regular permits; b) exploitation of minors without regular permits; c) exposure to situations of extreme danger.

- *"Illegal intermediation and exploitation of labour"* (Article 603 of the Criminal Code, as recalled in Article 25-*quinquies* of the Decree[49] which punishes those who take advantage of the workers' needy status and intermediate, use, hire or employ labour under conditions akin to exploitation. Situations such as the payment of remuneration that does not align with the labour union contracts, repeated violation of the working hours and rest regulations, violation of the occupational health and safety regulations are included among the exploitation indices.
- *"Racism and xenophobia"* (Article 604-*bis*, paragraph 3 of the Criminal Code, as recalled in Article 25-*terdecies* of the Decree), which punishes the instigation, provocation or propaganda that promote discrimination, or racial, ethnic, national or religious violence based on the denial or trivialization of the Holocaust or other crimes of genocide, war, or against humanity.

* * *

Section V - Offences relating to fraud in sporting competitions, illegal betting or gaming

Article 25-*quaterdecies* of the Decree refers to offences relating to fraud in sporting competitions, illegal betting or gaming and gambling using banned equipment. The offence of sports fraud is committed by anyone who offers or promises cash or other benefits or advantages to any participants in a sporting competition organised by a recognised federation, or who commits other acts of fraud for the same purpose. The same article also refers to offences and contraventions relating to the exercise, organisation or sale of lotteries, betting and gaming and the use of gaming machines in the absence of or in breach of the required licences or concessions.

7.5.2 Sensitive company activities

In the banking industry, the risk of offences being committed for the purposes of terrorism or subversion of the democratic order, or the risk of organised crime, transnational offences, offences against the person and offences relating to fraud in sporting competitions, the illegal exercise of betting or gaming, mainly relates to the opening of customer accounts, funds transfers, over-the-counter operations, and in particular, the lending process. For prevention purposes, these activities must be based on the principle of customer due diligence. This principle represents one of the key requirements established by Legislative Decree 231/2007 concerning prevention of the use of the financial system for the purpose of money laundering and of financing terrorism.

[49] The reiteration of Article 603-bis was added to Article 25-*quinquies* of the Decree by Article 6 of Law 199/2016, which is in effect from 4.11.2016.

The activities identified above are those where the risk of money laundering offences is also higher. Consequently, the control and conduct principles set out in the protocol concerning the financial fight against terrorism and money laundering are considered to be appropriate also for the purpose of preventing the above-mentioned offences.

Furthermore, the offences in this section also include:

- "*Inducement to withhold information or to make false statements to the judicial authorities*"; the company *activity* considered to be most sensitive in this respect is the management of disputes and settlements;
- "Employment *of foreign nationals with irregular permits of stay*", and "*Illegal intermediation and exploitation of labour*": *sensitive* activities regarding the former category are those pertaining to the recruitment and hiring of personnel, and for both categories, procedures relating to the purchasing of goods, services and consulting contracts.

Accordingly, for these offences reference is made to the protocols contained respectively in paragraph 7.6.2.1 "*Financial fight against terrorism and money laundering*", paragraph 7.2.2.6 "*Management of disputes and out-of-court settlements*", paragraph 7.2.2.10 "*Management of the staff selection and recruitment process*" and paragraph 7.2.2.8. *Management of the procedures for the procurement of goods and services and for the appointment of professional consultants.*

Such protocols also apply to the monitoring of any activities performed by Group companies or outsourcers on the basis of special service agreements.

7.6 Sensitive area concerning receipt of stolen goods, money laundering and use of unlawfully obtained money, goods or benefits, as well as self-laundering.

7.6.1 Types of offences

Introduction

Legislative Decree 231 of 21.11.2007, (hereinafter, the anti-Money Laundering Decree) and Legislative Decree 109 of 22.6.2007, which transposed Community law have strengthened the legislation on the prevention of the use of the financial system for the purpose of money laundering and on the fight against the financing of terrorism.

Article 25-*octies* of Legislative Decree 231/2001, introduced by the anti-money laundering Decree, extended the Entity's liability to cover the receipt of stolen goods, money laundering and unlawful use, even in the cases in which these acts are not committed for terrorist purposes or for subversion of the democratic order (covered by paragraph 7.5) or where they do not have the transnational characteristics provided for in the preceding provisions[50]. Finally Article 25-*octies* was amended adding the offence of self-laundering[51].

The reinforcing of the legislation on the administrative liability of Entities aims to prevent and combat more effectively the phenomenon of the introduction into lawful economic circuits of money, goods or other assets which are the proceeds of crime, as this hinders the activities of the justice system in detecting offences and prosecuting offenders, and in general damages the economic order, market integrity and free competition, by reason of the unfair competitive advantage enjoyed by those operators who have at their disposal financial resources of unlawful origin.

On a different plane, albeit still for the purpose of combating money laundering and of the financing of terrorism, but from another perspective, the anti-Money Laundering Decree establishes specific requirements for banks, financial intermediaries, and other specified obliged subjects (appropriate checks on customers; recording and storage of transaction documents; reporting of any suspicious transactions; notification of any infringements of the prohibitions concerning cash and bearer securities; reporting by the Entity's control and Audit Bodies of any infringements identified). Infringement of said obligations of itself but does not give rise to the Entity's administrative liability under Legislative Decree 231/2001, since such offences are not included in the list of the so-called predicate offences (i.e. the offences giving rise to the Entity's administrative liability) but is punished

[50] It should be noted that pursuant to paragraphs 5 and 6 of Article 10 of Law 146/2006, repealed by the anti-money laundering Decree, money laundering and unlawful use of money were considered to be offences giving rise to the liability of Entities only if the transnational characteristics laid down in Article 3 of the same Law were met.

[51] The new offence of self-laundering was introduced in the Criminal Code and added to the presumed crimes of Legislative Decree 231/2001 by Law 186/2014, that came into force on 1 January 2015.

pursuant to the anti-money laundering Decree, in accordance with a policy of preventive safeguards irrespective of whether money laundering offences are materially committed, to ensure compliance in all cases with the fundamental principles of in-depth knowledge of customers and the traceability of transactions, to avoid any danger that financial intermediaries might be unwittingly involved in illegal activities.

It should be noted that if the bank operator fails to perform his obligations being fully aware of the illegal origin of the goods subject of the transactions, he could be indicted for such offences, and consequently the Bank might incur administrative liability under Legislative Decree 231/2001.

Decree 195/2021 implementing Directive (EU) 2018/1673 on combating money laundering by criminal law through expanding the number of unlawful activities attributable to the predicate offences of receiving stolen goods, money laundering, the use of money, goods and benefits of unlawful origin and self-laundering which, in particular, now include *i)* offences committed intentionally *ii)* "violations", the latter on condition that they may be punished with a term of imprisonment of no more than 1 year or no less than 6 months.

The reform of offences extends the number of hypotheses in which an organization may be considered liable, as the types of conduct attributable to the commission of the predicate offences contemplated in Article 25 *octies* have increased, for example, an area in which the risks for the organization may have increased is occupational health and safety (Legislative Decree 81/2008).

The constituent elements of the offences in question are briefly illustrated below.

Receipt of stolen goods (Article 648 of the Criminal Code)

This offence occurs when any person, for the purpose of obtaining a profit for himself or for others, purchases, receives or conceals money or goods deriving from any crime whatsoever, in whose commission he did not participate, or in any case concurs in their purchase, receipt or concealment. In order for this offence to occur, the perpetrator must act with malice, i.e. knowingly and with the intent of obtaining a profit for himself or others, by purchasing, receiving or concealing stolen goods. Moreover, the offender must also be aware of the criminal origin of the money or the goods; the presence of this psychological condition can be signalled by serious and concurring circumstances: for instance the quality and the characteristics of the goods, the unusual economic and contractual terms and conditions of the transaction, the personal condition or employment of the holder of the goods – leading to the conclusion that the author of the act must have been certain of the illegal origin of the money or the goods.

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

This offence occurs where a person, who did not aid and abet commission of the underlying crime, substitutes or transfers money, goods or other assets deriving from a crime or carries out other transactions in respect of such money, goods or assets, so as to obstruct identification of their criminal origin.

The purpose of this provision is to punish those who – being aware of the criminal origin of the money, goods or other assets – perform the above-mentioned transactions, in such a way as to materially hinder discovery of the illegal origin of the goods in question.

For the offence to occur, the culprit needs not have acted for the purpose of obtaining some gain or of helping the perpetrators of the underlying crime to secure the proceeds of their crime. Money laundering consists of dynamic actions aimed at putting the goods into circulation, whereas their mere receipt or concealment could give rise to the offence of receipt of stolen goods. With regard to bank relationships, for example, the mere acceptance of a deposit could give rise to the replacement conduct which is typical of money laundering (replacement of cash with bank money, irrespective of the balance of the deposit).

Similarly to the offence of receipt of stolen goods, the offender's awareness of the illegal origin of the goods can be determined on the basis of any serious and univocal objective circumstance.

Use of money, goods or assets of illegal origin (Article 648-*ter* of the Criminal Code)

This offence occurs when any person uses money, goods or other proceeds of crime in economic or financial activities, with the exclusion of cases in which the perpetrator was also complicit with the underlying crime and with the exception of the offences set out in Article 648 (Receipt of stolen goods) and Article 648-*bis* (Money laundering) of the Criminal Code.

Compared with the offence of money laundering, while the same subjective element of awareness of illegal origin of the goods applies, Article 648-*ter* restricts the scope of this offence to cases in which such proceeds of crime are employed in economic or financial activities. However, given the comprehensiveness of the definition of the money laundering offence, it is hard to imagine any use of goods of illegal origin which would not fall under the scope of Article 648-*bis* of the Criminal Code.

Self-laundering (Article 648-ter.1 of the Criminal Code)

Anyone who, having committed or aided and abetted any crime that produces money, goods or other benefits, from said proceeds performs transactions, substitutes or transfers into economic, financial, entrepreneurial or speculative assets so as to obstruct their actual criminal origin is answerable to the offence of self-laundering.

This excludes liability to punishment of conduct consistent with the allocation of the illegal proceeds for the mere personal use or enjoyment. The sentence may be increased if the fact is committed when conducting professional, banking, or financial activity and may be reduced in the event of voluntary disclosure by the guilty party.

Remarks applying to the offences

Material subject

The material subject of these offences can consist of any asset having appreciable economic value and which may be exchanged, such as money, credit securities, means of payment, credit entitlements, precious metals/gems, tangible and intangible assets in general. These goods or assets must originate from the crime, i.e. they must be the product (the result or benefit obtained by the offender by committing the crime), the proceeds (monetary gain or economic benefit obtained from the offence) or the price (amount paid to induce, instigate, or lead someone to commit the offence). In addition to the offences typically aimed at the creation of illegal capital (for example, extortion in office, bribery, embezzlement, fraud, bankruptcy crime, arms or drug trafficking, usury, fraud against EU funds, etc.) and tax offences could also give generate to proceeds which are then laundered or of self-laundering, not only for fraud (for ex., the use of invoices for non-existent transactions that result in a fictitious credit; VAT to be deducted) but also in the case in which the economic utility consequential to a crime consists in a mere tax saving due to the non-disbursement of money originating from legal activities, (for example, failing to report or misreporting the income for amounts above the threshold of criminal relevance). The numerous violations[52] contemplated in Italian law (e.g. in the criminal code, in the Consolidated Law on Banking, Consolidated Law on Finance, in occupational health and safety laws and laws on the environment and waste), could constitute the background for committing the aforesaid offences.

Conduct and subjective element

A third party not involved in the original crime that generates illegal proceeds and who receives them from the original offender (or from others, however knowing of the illegal origin) to perform conduct thereupon provided for by the said crimes shall be answerable to the crimes of receipt, laundering or illegal reuse of stolen goods.

A party who provided any type of moral or material causal contribution to the commission of the original offence for example determining or strengthening the criminal intent of the original offender with the promise, even before the commission of offence, his help in the recycling/using the proceeds could instead be answerable to conspiracy in the crime that generated the illegal proceeds and, consequentially, also in the subsequent crime of self-laundering, should he carry out the conduct.

The crime of self-laundering, unlike as prescribed for crimes of money laundering and of unlawful use, requires that the conduct be characterized by methods suitable for the actual masking of the true criminal origin of the goods; the interpretation of the most innovative aspects of the law- that is to say requirement of the actual hindrance and the condition of non liability to punishment of the self-

[52] Including, as indicated in the introduction, conduct that may constitute the grounds for committing the offences of the receipt of stolen goods, money laundering, use of unlawfully obtained money, goods or benefits, as well as self-laundering.

launderer for personnel use (which would again seem to be excluded if the original offence and the reuse take place in the performance of a business activity) – shall necessarily refer to the jurisprudential applications of the crime.

As to the subjective element, as already stated, the offences in question must be marked by awareness of the fact that the goods in question are the proceeds of crime. According to a particularly strict interpretation, the offence may also occur if the person dealt with the goods while harbouring suspicions as to their illegal origin, accepting such risk ("dolus eventualis" or indirect intention). With reference to banking operations , it should be noted that the presence of anomaly indicators or anomalous conducts as set out in the measures and in the patterns issued by the competent Authorities (as concerns financial intermediaries, by the Bank of Italy and by the UIF (Unità di Informazione Finanziaria - Finance Intelligence Unit) in specific concrete situations might, if the particularly strict interpretation mentioned above is adopted, be considered as a serious and univocal objective circumstance which should give rise to doubts as to the illegal origin of the goods.

Correlations with the original offence related to the illicit gains.

The crimes of this Sensitive area subsists the cases in which the relative conduct is subsequent to the perfecting of the crime that was the origin of the illicit gains, even if performed after its extinction (for example due to the statute of limitation or death of the original offender), or also if the author of the crime is not chargeable or liable to punishment, or if the condition for prosecution do not exist (for example, no lawsuit has been filed, or upon request by the Minister of Justice, necessary to pursue common crimes common committed in foreign countries overseas, pursuant to articles 9 and 10 of the Criminal Code)[53].

7.6.2 Sensitive company activities

The risk of the commission in a banking environment of money laundering offences, understood in a broad sense (hence therein including self-laundering) appears more pronounced, being a typical risk of the banking and financial circuit, basically with reference to relationships with customers and in cases of involvement/aiding and abetting thereof; in particular, it concerns:

- the establishment and management of ongoing relations with customers;
- the transfer of funds;
- bank teller operations;

[53] With regard to the irrelevance of extinction of the offence that constitutes the grounds for another offence see Article 170, paragraph 1 of the Criminal Code; For the irrelevancy of the lack of a condition of liability to punishment or prosecutability, see Article 648, paragraph 3, of the Criminal Code, also cited by Articles. 648-*bis,* , 648-*ter* and 648-*ter.1* of the Criminal Code.

- trading in financial instruments.

Prevention activity is based on in-depth knowledge of customers and counterparties and on compliance with the legal requirements relating to the fight against money laundering and the financing of terrorism.

The central importance of strict compliance with the provisions dictated by the anti-money laundering Decree for the purpose of prevention the presumed crimes in question also follows from the subsequent considerations. It should first of all be stated that the Decree - for the purpose of identifying the type of conduct at risk for money laundering, and subject to the reporting requirements of suspicious transactions, defines, under Article 1 “transaction” as the transmission or the movement of means of payment” and contains a list, under Article 2, of conduct, characterized as money laundering, of very broad extension, so as to include conduct which, for criminal purposes, could include the commission of the crime of self-laundering, or the commission of other the predicated offences in question and that, if carried out by employees or by top-mangers, could entail administrative liability of the Entity itself. Finally, the above-mentioned list also includes atypical conduct relating to other offences, such as aiding and abetting an offender (Article 378 of the Criminal Code) which, where it is of a transnational nature (on this point see Chapter 7.5) can also constitute a predicate offence for the administrative liability of Entities.

The risk takes on different connotations and appears less relevant with regard to those bank transactions typical of a “company”, i.e. in those areas where the bank, apart from its core activities, carries out instrumental transactions, makes equity investments or carries out transactions on its own capital, and fulfils its accounting and tax requirements or requirements of specific sector regulations. In these areas in fact there is a well-developed articulation of control system and procedures already established by the legislation in the sector (for example Legislative Decree 81/2008, Legislative Decree 152/2006, etc.) and in that concerning listed companies, in order to ensure the observance of the principles of transparency, correctness, objectivity safeguards and the traceability of management.

We reproduce below the protocol laying down the control principles and rules of conduct applicable to the management of the risks relating to the financial fight against terrorism and money laundering. The protocols regulating other sensitive activities – such as Management of disputes and of out-of-court settlements (paragraph 7.2.2.6), Management of the procedures for the procurement of goods and services and for the appointment of professional consultants (paragraph 7.2.2.8); Management of gifts, entertainment expenses, donations to charities and sponsorships (paragraph 7.2.2.9); Management of real-estate and cultural assets (paragraph 7.2.2.11) and the Management of valuables (paragraph 7.3.2.1) – also include certain control and conduct principles based on the

same criterion of thorough assessment of suppliers, consultants and contractual counterparties in general, and which can also help prevent the offences addressed in this section.

More generally, all the protocols of this Model, where meant to prevent the committing of offences that can generate illicit gains, must also be understood to meant to prevent money laundering offences in a broad sense. We cite especially the protocols relative to the Sensitive areas concerning corporate offences - in particular, the protocol on the Management of periodic reporting (paragraph 7.4.2.2) - the offences and regulatory offences ascribable to market abuses and computer crime.

All the foregoing protocols are supplemented by detailed corporate regulations governing such activities and also apply to the monitoring of any activities performed by outsourcers or other Group companies on the basis of special service agreements.

7.6.2.1. Financial fight against terrorism and money laundering

Introduction

The purpose of this protocol is to define the roles, operational responsibilities and control and conduct principles relating to the financial fight against terrorism and money laundering. The protocol refers to applicable company provisions, and in particular the "Guidelines for combating money laundering and terrorist financing and for managing embargoes" and internal regulations applicable from time to time".

This protocol applies to all the Bank Structures involved in the sensitive activities identified above and in the control of the risks linked to anti-money laundering legislation.

The contents of this protocol are aimed at ensuring that the Bank complies with current legislation and the principles of transparency, correctness, objectivity, traceability and confidentiality in performance of the activity in question.

Process description

For the purposes of combating the financing of terrorism and money laundering, the following operational areas are pertinent:

- identifying and knowing the customers and the persons on behalf of whom they operate, assessing their risk profile, i.e. the likelihood of exposure to phenomena of money laundering activities financing terrorism by means of a specific profiling procedure. Risk assessment is based on knowledge of the customers and takes into account, in particular, objective aspects (which type of activity the customers carry out, which transactions they perform and which instruments they use[54]) and subjective aspects (persons subject to strengthened control requirements; entities connected with Countries that have shortcomings in the oversight of money laundering or critical aspects in terms of tax cooperation, etc.). Particular attention must be paid to detecting any possible involvement in transactions or in relationships with persons (both natural and legal persons) that are included in public lists published both at national and international level (UN, EU, OFAC lists, etc., hereinafter collectively referred to as "the Black Lists";
- opening of new ongoing relationships and updating/review of the information on existing customers, to ensure compliance with the principle of the "know your customer" rule;
- granting and management of credit lines to customers (credit process);
- monitoring of operations and ongoing assessment of the risk of money laundering or financing of terrorism, based on specific timelines and procedures defined according to risk profile levels;

[54] For instance, the interposition of third parties, the use of corporate, associative or trust instruments likely to limit transparency with regard to the ownership and management structure; use of cash or bearer instruments

- assessment of the transactions ordered by customers with persons/Countries/goods which are subject to financial restrictions (freezing of assets and resources, prohibition of financial transactions, restrictions on export credit or investment) and/or commercial restrictions (general or specific trade sanctions, bans on imports and exports - for example, an arms embargo);
- discharge of regulatory obligations on the retention and availability of documents, data and information to combat money laundering and terrorist financing;;
- external reporting to the Supervisory Authorities and internal reporting for the purpose of preparing the external reports.

The operating procedures for management of the above-mentioned processes are governed by the internal rules, which are developed and updated by the competent Structures. Such internal rules form an integral and substantive part of this protocol.

Control principles

The control system for monitoring the processes described above is based on the following elements:

- Clearly defined responsibilities:
    - the internal set of rules identifies the individuals and Structures responsible for initiating//managing/controlling the processes described above;

- Segregation of duties:
    - as to ongoing relationships relating to the disbursement of credit, the credit application assessment procedure shall be performed by different individuals from those empowered to approve granting of the financing, excluding those exceptions expressly set out in the internal rules applicable from time to time;
    - in the situations defined by law and by the internal rules where strengthened obligations to carry out thorough customer assessment apply, the opening of new relationships, maintaining of existing relationships and the performance of transactions shall be subject to issue of authorisation by a different Structure from the operational one;
    - with regard to the monitoring of operations in order to identify potentially suspicious transactions, segregation of duties shall be organised as follows:
        - the operators of Local Branches or other operational Structures shall monitor the transactions falling under their remit, and shall report any suspicious transactions to their respective Structure Manager for further assessment and/or reporting;
        - the operational Structure Manager, based on the information available to him, or on reports received from his collaborators, from Managers of other non-operational Structures or from the Gianos procedure (“unexpected” transactions) shall, if the

transaction is found to be suspicious, report it to the Manager in charge of reporting on suspicious transactions;

- such Manager responsible for reporting suspicious transactions shall analyse the report so received and shall autonomously carry out the necessary investigations on the suspicious transaction, deciding whether or not the reports should be forwarded to the competent Authority.

- Control activities: the control system for monitoring the processes described above is based on the following elements:
  - as part of comprehensive customer profiling, at the time of entering into a contractual relationship, the Head of each operational Structure shall verify, using a risk-based approach, the correctness and completeness of customer identification details, and shall check the information acquired on the customer's economic activity; this information must be periodically updated, with reference to the economic reasons for requested or executed transactions;
  - at the time of recording the customers' identification details and then on a periodical basis, their names shall be checked against the updated specific "Black Lists" to ensure they do not appear thereon;
  - as part of the procedures for granting and managing credit lines to customers, the consistency between the requested financing and the customer's economic-financial profile shall be checked, in order to assess any (potential) exposure to money laundering or terrorism financing phenomena;
  - medium and long-term monitoring by the competent operational Structures to provide cross-checks between the customer's subjective profile, the type of transaction, the frequency and manner of execution, the reference geographical area (with particular regard to operations from/to Countries at risk) as well as the risk level assigned to the product subject of the transaction, the funds used, the timeframe of the investment, the conduct adopted by the customer at the time of executing the transaction (if the transaction is performed in the customer's presence);
  - monitoring and control by the Structures tasked with internal controls of the precise performance of the operational Structures' activities concerning:
    - acquiring the information necessary to identify and profile customers;
    - assessing the transactions highlighted by the Gianos procedure (or by other IT procedures in use);
    - detecting and assessing any other indicators of abnormality which might occur in actual operations;
    - detecting any infringements of the regulatory limits on the use of cash and bearer securities;
    - recording relationships and transactions in the Financial Transaction Database (AUI - Archivio Unico Informatico) and filing documents and information;
  - all ongoing contractual relationships and transactions involving the transmission of means of payment must be processed with methods enabling their procedural recording in the Financial Transaction Database with correct and complete data, also using automated data quality

controls. To this end, any transactions or relationships that are listed as “suspended” must be “supplemented” and “regularised” within the time limits required by the procedures and in any case within the time limits set out in applicable laws or regulations;
  - the correct performance of all requirements shall also be monitored in respect of the activities of foreign branches;
  - computer control systems are adopted to prevent operations from concerning persons/Countries/goods which are subject to financial restrictions (freezing of assets and resources, prohibition of financial transactions, restrictions on export credit or investment) and/or commercial restrictions (general or specific trade sanctions, bans on imports and exports - for example, an arms embargo).

- Process traceability including both the electronic and the paper trail:
  - in order to allow reconstruction of responsibilities and of the reasons for the choices made, the Structure from time to time concerned shall be responsible for filing and storing, also in telematic or electronic format, all the documentation it produces relating to performance of the requirements associated with the process described; in particular:
    - the Branch manager or the customer relationship manager shall keep in confidential and orderly files all the documentation pertaining to customer identification and profiling;
    - all the documentation pertaining to operations and to the periodic checks carried out on customers' accounts shall be systematically filed by the competent operational Structures;
    - full records shall be kept of the decisions and of any stated underlying reasons for altering a customer profile and for a consequent decision on whether or not to report a transaction as suspicious.

- Information shall be kept confidential, in particular that concerning identification of real account holders, customer profiling and the processes for monitoring transactions and reporting suspicious transactions, by adopting appropriate IT and physical measures ensuring such confidentiality.

- Training: activities specifically focused on continuous training of employees and collaborators in identifying the risk profiles associated with the legislation on anti-money laundering and combating terrorism financing shall be provided on a regular basis.

Rules of Conduct

The Bank Structures which are howsoever involved in the financial fight against money laundering and financing of terrorism shall comply with the procedures set out in this protocol, the applicable provisions of law, the internal rules and any provisions of the Group's Code of Ethics and Internal Code of Conduct.

In particular the competent Structures have an obligation to:

- ensure the development and implementation of the applications used in the financial fight against terrorism and money laundering and in any case in all the activities based on “appropriate knowledge of customers”;
- verify and ensure the dissemination among the Bank’s structures of the restrictive measures – containing operational limits in specific areas – issued by EU, OFAC - and of the updated “Black Lists”, together with the adoption of automatic detection procedures;
- ensure that customers operate in compliance with the restrictions and the authorizations provided for by the embargo measures or by the rules governing the export of particular types of goods and/or materials (e.g. dual-use goods, hazardous chemical substances);
- establish detailed rules of conduct in the internal regulations/operating rules, supplementing and expanding on the external legislation and the principles laid down in this protocol;
- where the customer or transaction assessment involves more than one operational Structure or Group company, the Structures or companies concerned shall co-operate with each other and, where allowed by current legislation, shall exchange information for the purpose of acquiring comprehensive and appropriate knowledge of the customer and of the typical transactions he engages in;
- in relations with foreign correspondent banks, documentation shall be obtained whereby such correspondent banks declare they have fulfilled anti-money laundering obligations and/or the obligations set out in the laws of other Countries (in particular the United States of America);
- ongoing and systematic training and updating shall be delivered to staff on anti-money laundering legislation and embargoes and on the aims pursued by such provisions;
- the reference legislation and all updates thereof shall be disseminated to all employees, regardless of their actual duties.

Furthermore, all bank employees and collaborators (including Financial Advisors), acting in compliance with company procedures must:

- at the time of activating ongoing contractual relationships or executing transactions which exceed the legal threshold:
    - identify the customer and verify whether his name appears on the latest edition of the “Black Lists”;
    - verify the identity of actual account holders, obtain information on the purpose and nature of the relationship or transaction and, where the customer is a company or an Entity, verify that the person requesting the transaction holds due authority to sign, and check the customer’s ownership and control structure;
    - carry out customer profiling;
- regularly update all data concerning ongoing relationships to allow continuing assessment of the customer’s economic and financial profile;
- perform the customer verification and profiling process where, regardless of any applicable amount threshold or exemption, suspicions of money laundering or of the financing of terrorism are harboured, or doubts arise as to the truthfulness or adequacy of already acquired identification details;

- keep information concerning the anti-money laundering risk level assigned to the customer and the relevant score calculated by the procedure strictly confidential; such information will not be disclosed to customers under any circumstance;
- actively participate in the processes of detecting and reporting suspicious transactions;
- consider whether to initiate a reporting process where abnormal indicators are detected, even if such abnormalities were not signalled by IT procedures, or where it is impossible to comply with the appropriate verification requirement;
- verify whether the customer's name appears on the latest version of the "Black Lists" and block or, in any case, refrain from executing transactions concerning persons/Countries/goods subject to financial restrictions (freezing of assets and resources, prohibition of financial transactions, restrictions on export credit or investment) and/or commercial restrictions (general or specific trade sanctions, bans on imports and exports - for example an arms embargo) or which are howsoever suspected of having connections with money laundering or the financing of terrorism;
- report any infringements of the regulatory limits on the use of cash and bearer securities detected in customer transactions;
- strictly comply with the internal procedures on the recording of relationships and transactions in the financial transaction database (AUI) and on the filing of data, information and documentation.

The Bank employees, whether they operate from the central Structures or the local branches, in charge of the assessment and authorization activities set forth by the anti-money laundering processes, must exert their discretion according to professionalism and reasonableness. In the event of personal or corporate conflicts of interest, even if potential, they must:

- Immediately report to their manager about the conflict of interest detailing its nature, terms, origin and relevance;
- Refrain from assessment/authorization activities, delegating decisions to their manager or to the appropriate Structure as defined by the internal regulations. By way of example, conflict of interest may occur if personal interests interfere (or seem to interfere) with the Company's or the Group's, thus hindering the effective and impartial performance of one's activities, or if inappropriate personal benefits are pursued based on the position held within the Company or the Group.

Employees are furthermore forbidden to inform, even unintentionally, third parties (including their family members, close relations or their family's close relations) about the result of any assessment/authorization activity in any circumstance not provided by the law for reasons other than those pertaining to office activity.

In any case, it is forbidden to engage/collaborate in or induce conduct which may belong to one of the types of offence covered by Legislative Decree 231/2001; more specifically, purely by way of example and without limitation it is forbidden to:

- set up ongoing relationships, or maintain existing ones, and execute transactions when it is impossible to fulfil the obligation of appropriately checking the customer's details, for instance when the customer refuses to provide requested information;
- execute transactions which are suspected of being linked to money laundering or terrorism financing schemes;
- receive or conceal money or assets obtained through any criminal act, or carry out any activity which may facilitate the purchasing, receipt or concealment of such proceeds of crime;
- replace or transfer money, goods or other assets originating from offences, or execute any other transactions in respect of such assets which might obstruct identification of their criminal origin;
- take part in one of the acts listed in the above bullet points, conspire with others to commit them, attempt to commit them, aid and abet, instigate or advise anyone to commit them or assist in their execution;
- make available to customers who belong to or are howsoever close to criminal organisations any services, financial resources or other economic means which may be instrumental to the pursuit of illegal activities.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.7 Sensitive area concerning offences against cultural assets

7.7.1 Types of offences

Introduction

Law 22 of 9 March 2022, in the context of previously existing legal reform, allocated offences previously contained in the Code of Cultural Assets (Legislative Decree 42/2004) to the Criminal Code, also adding new cases, and introduced in Legislative Decree 231/2001, Article 25 septiesdecies "Offences against cultural assets" and Article 25 duodevicies "Laundering of cultural assets" and the destruction and looting of cultural and landscape assets".
The offences in question are described below.

Theft of cultural assets (Article 518 *bis* of the Criminal Code)

Anyone who takes possession of a cultural asset belonging to others, removing it from them, in order to gain a profit, for themselves or others, or who takes possession of cultural assets belonging to the State, found in the subsoil or on the seabed will be punished.

Misappropriation of cultural assets (Article 518 *ter* of the Criminal Code)

Anyone who, has possession of a cultural asset, that appropriates it in order to gain an unjust profit for themselves or others, will be punished.

Handling stolen cultural assets (Article 518 *quater* of the Criminal Code)

Anyone who acquires, receives or conceals cultural assets originating from any crime or in any case that are involved in such an activity, in order to gain a profit for themselves or others, will be punished.

Forging documents relating to cultural assets (Article 518 *octies* of the Criminal Code)

The crime punishes anyone who, wholly or in part, forges a document or, alters, destroys, eliminates or conceals a true document relating to cultural assets, in order to make their origin appear to be lawful, and also anyone who uses said, without contributing to realising or altering the document.

Violations concerning the disposal of cultural assets (Article 518 *novies* of the Criminal Code)

The conduct of the owner of cultural assets that transfers said or puts them up for sale without authorisation where required or delivers the good within the time frame of 60 day envisaged for pre-emption by the State or that materially transfers said without presenting the related notice, where required, will be punished.

Illegal import of cultural assets (Article 518 decies of the Criminal Code)

The crime punishes anyone who, apart from cases of aiding and abetting in the crimes contemplated in Articles 518 quater, 518 quinquies, 518 sexies and 518 septies, imports cultural assets originating from crime or found following searches carried out without authorisation, or required by State regulations applicable where items are found, or exported by another State in violation of the law on protecting cultural assets of that State.

Outflow or illegal export of cultural assets (Article 518 *undecies* of the Criminal Code)

The conduct of anyone who transfers cultural assets, assets of artistic, historic, archaeological, ethno-anthropological, archive and bibliographic interest or other items identified by specific regulations pursuant to laws on cultural assets, without the free transit declaration or export licence. The following are also punished:

- anyone who does not return to national territory, at the end of the deadline, cultural assets, assets of artistic, historic, archaeological, ethno-anthropological, archive and bibliographic interest or other items identified by specific regulations pursuant to laws on cultural assets, which have been authorised for temporary export or outflows, will be punished:
- anyone who makes statements that are untruthful in order to demonstrate to the competent export office, pursuant to law, that items of cultural interest are not subject to authorisation to leave national territory, will be punished.

Destruction, dispersion, deterioration, disfigurement, dirtying and unlawful use of cultural and landscape assets" (Article 518 *duodecies* of the Criminal Code)

Anyone who destroys, causes the dispersion, deterioration or makes wholly or in part own or others' cultural or landscape assets unusable and who, apart from the previous cases, disfigures or defaces own or others' cultural or landscape assets, or assigns cultural assets for a use which is incompatible with their historic or artistic nature or harms their conservation or integrity will be punished.

Forgery of works of art (Article 518 *quaterdecies* of the Criminal Code)

The following conduct will be punished:

- anyone, who in order to realise a product, counterfeits, alters or reproduces a painting, sculpture or graphic work or an antiquity or item of historic or archaeological interest;
- also without aiding and abetting in the forgery, alteration or reproduction, anyone who puts on sale, holds for sale, introduces for this purpose into the territory of the State or in any case circulates, as authentic, counterfeit, altered or reproduced paintings, sculptures or graphic works, antiquities or objectives of historic or archaeological interest;
- anyone knowing the forged nature, authenticates works or items (indicated in the first two sub
- through other statements, reports, publications, the affixing of stamps or labels or with any other means, confirms or helps to confirm, knowing the forged nature, as authentic, works or items (indicated in the first two subsections), that have been counterfeited, altered or reproduced; sections), that have been counterfeited, altered or reproduced.

Laundering of cultural assets (Article 518 sexies of the Criminal Code)

Anyone who, apart from cases of aiding and abetting the commission of the offence, transfers cultural assets from an unintentional offence or carries out other transactions, so as to obstruct identification of their criminal origin, will be punished.

Destruction and looting of cultural and landscape assets (Article 518 terdecies of the Criminal Code)

Anyone who carries out the destruction or looting of cultural or landscape assets or of cultural institutions and places will be punished.

7.7.2 Sensitive company activities

With the extension of the entity's liability to also cover crimes against cultural and landscape heritage, the legislator has aimed to extend the protection of these assets.

Within the Bank, the risk of committing these crimes could occur in managing the Bank's own cultural assets, for example in the case of cultural assets leaving/returning to the national territory without the required authorisation.

With reference to banking activities, the risk of committing offences against cultural assets could occur in relationships with customers, with respect to granting loans or providing services in favour of persons involved in the illegal activities in question (for example the building of golf courses or resorts in protected areas), that affect the landscape heritage of specific places.

Reference is made to the applicable protocols in:

- paragraph 7.2.2.3 "Management of the activities relating to the request for authorisation or fulfilment of requirements towards the Public Administration";
- paragraph 7.2.2.11 "Management of property and cultural assets";
- paragraph 7.6.2.1 on the "Financial fight against terrorism and money laundering".

Such protocols also apply to the monitoring of any activities performed by Group companies and/or outsourcers on the basis of special service agreements.

7.8 Sensitive area concerning crimes and administrative offences relating to market abuse

7.8.1 Types of offences

The Finance Consolidation Act governs the offences of "*Insider trading or unlawful disclosure of inside information", "Recommending or inducing others to commit insider trading" and "Market manipulation",* which are governed respectively by Articles 184 and 185.

Articles 187-*bis* and 187-*ter* of the Finance Consolidation Act include the administrative offences of "*Abuse and disclosure of insider information*" and of "*Market manipulation*", for which the illegal acts are essentially the same as for the previous two offences.

The responsibility of the Entity in whose interests these two criminal offences were committed is punished by Legislative Decree 231/2001 (Article 25-*sexies*), while for the two administrative offences, the responsibility derives from the Finance Consolidation Act (Article 187-*quinquies*) which is based on the same principles, conditions and exemptions as Legislative Decree 231/2001, except that for these administrative offences, the Entity will be liable whenever it is unable to provide proof that the perpetrator of the offence acted only in his or her interests or in the interests of a third party.

The offence of market rigging is also related to the area of market abuses in the broad sense (it is included among corporate offences: see paragraph 7.4.1), and it relates to unlisted financial instruments or those for which no application was made for admission to trading on a regulated market.

The above-mentioned rules are aimed at ensuring the integrity, transparency, correctness and efficiency of the financial markets, in accordance with the principle that all investors should operate on a level playing field with regard to access to information, knowledge of the pricing mechanism and knowledge of the source of publicly available information.

The rules for implementing this principle and for the repression of related offences are laid down in EU legislation, most recently in Directive 2014/57/EU (MAD II) and Regulation (EU) 596/2014 (MAR); Legislative Decree 107/2018 and Law 238/2001, in force since 29 September 2018, and 1 February 2022 respectively, which also covers this area and amends the disciplinary provisions of the Finance Consolidation Act mentioned above. Except for what is specified below with reference to each of the various offences, the punishable conduct may relate to[55]:

1) financial instruments admitted to trading or for which an application has been submitted for admission to trading on a regulated Italian or other EU market;
2) financial instruments admitted to trading or for which an application has been submitted for admission to trading on a multilateral trading facility (MTF) in Italy or another EU country;

[55] Under Article 183 of the Finance Consolidation Act, the regulation of market abuses does not apply to monetary management and public debt activities, nor activities relating to climate policy, in compliance with exceptions in Article 6 MAR, nor to own-share buyback schemes or schemes to stabilise securities prices, in accordance with the rules in Article 5 MAR.

3) financial instruments traded on an organised trading facility (OTF) in Italy or another EU country;
4) other financial instruments not covered by the above subparagraphs, which are traded outside of the above-mentioned trading facilities (OTC), whose price or value depends on the price or value of one of the instruments traded on the platforms referred to above, or which have an effect on them, including credit default swaps and contracts for differences (CfDs);
5) spot commodity contracts which are not wholesale energy products, suitable for causing a considerable change in the price or value of the above financial instruments;;
6) financial instruments, including derivative contracts or derivative instruments for the transfer of credit risk, suitable for causing a considerable change in the price or value of a spot commodity contract, if the price or value depend on the price of value of said financial instruments;
7) benchmarks;
8) conduct or transactions, including offers, relating to auctions on authorised auction platforms, such as a regulated market trading emissions allowances or other related auction products, even when the auction products are not financial instruments, pursuant to *Commission Regulation (EU) No 1031/2010 of 12 November 2010*.

Specifically:

- the provisions in Articles 184, 185, 187-bis and 187-ter apply to facts concerning financial instruments, conduct or transactions indicated in numbers 1), 2) 3), 4) and 8);
- the provisions in Articles 185 and 187-ter apply to facts concerning spot commodity contracts, financial instruments and the benchmarks indicated in numbers 5), 6) and 7).

Under Article 182 of the Consolidated Finance Act, the offences are punishable under Italian law even if committed abroad (e.g. in a foreign Branch of the Bank), where these offences involve financial instruments admitted to trading, or for which admission to trading has been requested, on an Italian regulated market or on an Italian MTF, or if they relate to financial instruments traded on an Italian OTF.

Under Article 16 of the MAR, market operators and investment firms who manage a trading facility and who prepare or execute trading operations on a professional basis are required to adopt effective systems, devices and procedures[56] to prevent, identify and immediately report any suspicious orders or transactions to the relevant authorities, if they could amount to insider trading or market manipulation, or even attempts at such offences.

The violation of these obligations is regulated by Article 187b(1) of the Finance Consolidation act; A failure to report any violations may, in theory, expose the Bank to involvement in the offence committed by the customer, depending on the circumstances and methods surrounding the operation.

The offences are described below.

[56] The reporting procedures are defined by CONSOB in Article 4-*duodecies* of the Finance Consolidation Act, in accordance with the rules on internal whistleblowing systems.

Insider trading or unlawful disclosure of inside information. Recommending or inducing others to commit insider trading (Article 184 of the Finance Consolidation Act)

This offence punishes anyone who directly or indirectly misuses inside information they have received (i) because they are a member of the Board of Directors, management or control body of the issuer; (ii) because they participate in the capital of the issuer; or (iii) because they hold a position or function in relation to their working or professional activities; (iv) as a result of the preparation or commission of a crime (e.g. " *Intrusion into a computer system and extraction of inside information* "); (v) for reasons other than those listed.

Any of the above-named persons commits an offence if:

a) who buys, sells or carries out other operations[57] on financial instruments either directly or indirectly on their own account or on behalf of a third party, using that information (insider trading);
b) discloses that information outside of the normal exercise of their work or professional or outside of a market survey in accordance with Article 11 (tipping);
c) recommends to, or induces other people to carry out any of the above operations in letter a), on the strength of that information (tuyautage).

Insider information means information "*of a specific nature which has not been made public*[58] *and which concerns, directly or indirectly, one or more issuers of financial instruments or one or more financial instruments which, if made public, may have a significant impact on the prices of those financial instruments or on the prices of related derivatives*[59]".

Insider information may also relate to: i) commodities derivatives; ii) related spot commodity contracts; iii) greenhouse gas emissions allowances or other related products; iv) information provided by the customer in connection with pending orders in the customer's financial instruments, which if made public may have a significant effect on the prices of such instruments, on the connected spot commodity contracts or on the connected derivatives.

In the context of the Bank's typical operations, there are various cases in which the Bank could be held liable if the offence was committed entirely or partially in its interests. This risk may exist, for example, in relation to proprietary trading, when the person who orders or executes the operation misuses insider information about a certain issuer to which the Bank has access during the course

[57] This also includes operations to cancel or amend a previous order that was given before having access to the inside information.

[58] Article 17 MAR provides for the cases, times and terms regarding the obligation on the part of the issuer of financial instruments or participants in the market for greenhouse gas emissions quotas, to disclose insider information to the public.

[59] The definition of inside information is established by Article 180, paragraph 1, letter b-ter of the TUF, by simple reference to Article 7, paragraphs 1 to 4 of the MAR. Reference should be made to this provision for a detailed reconstruction, in particular regarding the concepts of "precise nature" and "significant effect".

of its activities as there are multiple accounts held with the issuer, or in relation to what is known as "front running"[60], in which case information relating to a customer's pending orders is also considered to be insider information. A special case may exist where a member or employee of the Bank is a member of executive bodies in other companies, and exploits insider information obtained from the other company, in the interests of the Bank.

Market manipulation (Article 185 of the Finance Consolidation Act)

This criminal offence occurs when a person disseminates false information or sets up sham transactions or employs other devices likely to produce a significant alteration in the price of financial instruments[61].

There is no punishment for orders for sale and purchase or other operations which, although having the potential to give misleading signals to the market or to artificially set the price, are justified by legitimate reasons and which were carried out in accordance with market practice permitted by the regulator responsible for the reference market according to Article 13 of the MAR.

In the context of the Bank's typical operations, there are various cases in which the Bank could be held liable if the offence was committed entirely or partially in its interests. The risk may take the form of manipulation of information (for example by distorting the use of marketing communications or other promotional and commercial information relating to issuers of financial instruments and/or listed financial instruments), or in the various forms of manipulation in the context of the Bank's activities in proprietary trading on the financial markets, in direct trading with customers, market making, etc.

Administrative sanctions: insider trading and market manipulation (Article 187-*bis* and Article 187-*ter* Consolidated Law on Finance)

As stated above, specific administrative sanctions have been introduced to punish the same material acts which give rise to both types of criminal offence (Articles 184 and 185 of the Consolidated Law on Finance).

The administrative offences governed by Articles 187-*bis* and 187-*ter* of the Finance Consolidation Act do not describe the prohibited conduct but simply refer to the prohibition on the abuse or unlawful disclosure of insider information and market manipulation, as defined in Articles 14 and 15 of the

[60] Front running means exploiting inside information on still to be executed customer orders for the benefit of the intermediary or for the benefit of another customer while also pursuing the intermediary's interest or benefit.

[61] For a more detailed description of the operations and systems that can give false or misleading information to the market or which set the market price at an irregular level, see Article 12 and Annex I of the MAR, which contains a non-exhaustive list of indications of manipulation consisting of the use of false or misleading information, in price setting and in the use of false instruments or other devices.

MAR[62]. The reference to the definitions of the cases contained in European legislation also entails a generic reference to the other MAR provisions that define the concepts of abuse, illegal communication and manipulation, and which are also the reference source for the crimes illustrated above, even though no express reference is made.

This does not rule out the possibility of the same person being prosecuted and punished for the same acts, with cumulative proceedings and punishments for the crime and for the administrative offence: in such a case, Article 187-*terdecies* of the Finance Consolidation Act provides that the legal authorities and Consob need to take into account - when issuing the penalties against the individuals who committed the offences and the entities who are liable for the criminal and administrative offences committed by their employees or executives - any sanctions already imposed during the criminal or administrative proceedings that were concluded first, and that in any case the second fine may only be imposed for the amount in excess of the first fine[63].

7.8.2 Sensitive company activities

The sensitive activities identified by Model which involve the highest risks of crimes and administrative offences relating to market abuse are the following:

- Management and disclosure of information and of external communications for the purposes of prevention of criminal and administrative offences in the area of market abuse;
- Managing orders and market transactions to prevent administrative and criminal offences linked to market abuse.

We reproduce below, for each of the above-mentioned sensitive activities, the protocols laying down the control principles and rules of conduct applicable to these activities, as well as the detailed corporate regulations governing such activities.

[62] The liability of the entity for the administrative offence committed by its employees or top management is also indicated in Article 187- *quinquies* of the TUF by referring to the violation of the prohibitions referred to in Articles 14 and 15 of the MAR. A pecuniary sanction from €20,000 to €15 million is envisaged for the entity, or up to 15% of turnover, if this is greater than €15 million. The punishment will be increased to up to ten times the product or proceeds of the offence, if of a large amount. In addition, the product or proceeds of the administrative offence will be confiscated.

[63] The entity may thus be liable both for the administrative offences or crimes, and for the criminal offences charged to an employee, for the same events. The sanctions imposed on the entity for the administrative offences indicated in the above note could thus be added to the punishment for criminal offences as provided for in Article 25-sexies of Legislative Decree 231/2001, namely a fine of up to €1,549,000, increased up to ten times the product or proceeds that were obtained, if of a large amount.

Such protocols also apply to the monitoring of any activities performed by Group companies or outsourcers on the basis of special service agreements.

7.8.2.1. Management and disclosure of information and of external communications for the purposes of prevention of criminal and administrative offences in the area of market abuse

Introduction

This protocol applies to all members of the Bank's Corporate governance bodies and to all the Bank's employees and external staff with access to inside information, in the meaning provided by current legislation and regulations, or who handle the Bank's communications to the market and, in general, all external communications, including the publication of studies and recommendations and any dissemination of news, data or information in the framework of business relations, of marketing or promotional activities, relations with the media, as well as compulsory "price sensitive" communications.

The process of managing and handling inside information could present opportunities for the commission of the criminal offence of insider trading or unlawful disclosure of inside information or of the corresponding administrative breach, set out respectively in Articles 184 and 187-*bis* of the Finance Consolidation Act.

Sound management of this process also goes to prevent the offences of market rigging and market manipulation and their corresponding administrative breach - respectively set out in Article 2637 of the Civil Code and in Articles 185 and 187-*ter* of the Finance Consolidation Act – with regard to "information manipulation", ensuring adequate control of the potential risk of "dissemination of false or misleading information, rumours or news".

As concerns prevention of "operational manipulation" reference is made to the protocol set out in paragraph. 7.8.2.2, on "*Management of orders and market transactions to prevent the crimes and administrative offences relating to market abuse*".

The purpose of the rules set out in this document, in compliance with the requirements of current legislation, is to ensure that:

- information is circulated within the company without affecting its privileged or confidential status and all safeguards are adopted to prevent disclosure of such information to unauthorised persons and to ensure that disclosure of inside information to the market is effected in a timely and complete manner and in any case in such a way as to avoid inequalities among the public in access to information;
- inside information is not disclosed, even unintentionally, to third persons for reasons not related to the office activity, prescribing to this purpose a particularly cautious conduct to employees and to the members of the Corporate governance bodies and furthermore, for employees, the duty to report to the Bank's competent Structures those situations that might involve the risk of an unauthorized disclosure of such information;

- the Corporate governance body members, the employees and the collaborators do not misuse inside information available to them by virtue of their position and/or their functions within the bank for the purpose of operating in financial instruments in the interest and on behalf of the Bank and/or their own;
- the Bank's communications to the market and, in general, to external parties are made by clearly identified and duly empowered persons, to prevent the disclosure of false or misleading information or news concerning either the Bank or third companies.

The Intesa Sanpaolo SpA Group Regulation for the management of inside information provides for the adoption of internal organizational measures aimed at the management and timely disclosure to the public of inside information concerning it directly, in compliance with the provisions in Articles 17 and 18 of the MAR. In particular, the organizational, management and control measures of inside information are aimed at ensuring conditions of correctness, efficiency and timeliness in the transparency of the Bank's disclosure, as well as the methods of handling information that could have a significant effect on the prices of the financial instruments issued by the Bank and traded on relevant markets or even on the prices of related derivative financial instruments.

The definitions given in this protocol are aimed at ensuring the Bank's compliance with applicable regulations and principles of transparency, correctness, objectivity and traceability in carrying out the activities concerned.

Process description

The process of managing and disclosing the inside information of which the Bank's structures become aware is organised in accordance with the specific operational responsibilities assigned under the Bank's role and mission allocation system.
The criteria used for identifying inside information and relevant information (as defined in the Consob Guidelines of 13 October 2017 on the management of insider information), and the operating procedures for managing that information are governed by the internal rules developed and updated by the competent Structures which form an integral and substantial part of this protocol.

By reason of their operational duties and functions within corporate operations, the Bank's Structures may handle inside information concerning:

- the Bank, its subsidiaries and the financial instruments issued by each of these companies;
- the customer companies and the financial instruments they issue (e.g. when providing corporate finance services to listed customer companies);
- derivatives on commodities pertaining to the connected spot commodity contract;
- emissions quotas or related auction products;

- information provided by a customer and/or relating to pending customer orders, of a specific nature which has not been made public and which concerns, directly or indirectly, one or more issuers of financial instruments or one or more financial instruments which, if made public, may have a significant effect on the prices of those financial instruments or on the prices of related derivatives (significant in the case of front running).

The relevant information and inside information is identified on the basis of the criteria set out in the relevant Group regulations. It may concern an internal decision of the Bank (for example strategic initiatives, agreements and extraordinary transactions) or be obtained with regards to objective events or circumstances having an impact on the business activity and/or on the performance of the financial instruments it has issued (for example period financial statements, information on the management) or be acquired in the course of activities performed in the name or on behalf of third-party companies or from activities performed on financial markets on one's own or third persons' behalf.

Inside information relating to third-party issuers or financial instruments issued by them may also derive from operations relating to both investment services and activities, and activities on the primary market and ancillary services (corporate finance, in particular such as advisory services, M&A and extraordinary transactions concerning the issuer's capital or debt structure, etc.) when provided to issuers of listed financial instruments, or to issuers of financial instruments for which admission to trading on a regulated market has been requested, or issuers of financial instruments. admitted to trading on an MTF or OTF, or for which a request for admission to trading on an MTF has been submitted.

In order to ensure the traceability of access to inside information, pursuant to Article 18 MAR, Registers of Intesa Sanpaolo S.p.A. of persons having access to inside information have been created – covering access to both inside information concerning the Bank, and information concerning third party issuers in whose name or on whose behalf Intesa Sanpaolo S.p.A. operates; a similar register has also been created for each of the Group Companies to which the relevant legislation applies; for other inside or confidential information falling outside the scope of Article 18 MAR and of the relevant implementation rules, the Bank has also created a supplementary system for recording sensitive situations within its internal regulations, consisting of the watch list and the limited information list.

In order to ensure that the disclosure to the market of information which is price sensitive for the Group, i.e. information on events which take place within the scope of the activities of the Parent Company and/or of its Subsidiaries and which have a substantial impact on the Group's profit and

loss performance and asset situation, takes place in observance of the law, the Bank has created an internal set of rules covering the following phases:

- identifying and monitoring of inside information;
- preparing and approving the communication to be made to the market;
- issuing of a statement by the Manager responsible for preparing a company's financial reports, pursuant to Article 154-*bis* of the Finance Consolidation Act, if the communications concern directly the Bank's and the Group's economic and financial reporting information;
- the public disclosure of inside information.

With regard to further obligations of correctness and transparency in the disclosure of news, data and information, even concerning third party issuers, the Bank in order to prevent any manipulation of information has adopted internal rules governing the process of disclosing studies and recommendations which comprises the following phases:

- preparing the recommendations;
- monitoring compliance with the adopted standard;
- disclosing the recommendations.

Control principles

The control system for monitoring the processes described above is based on the following elements:

- creation of the Register of persons having access to inside information pursuant to Article 18 of the MAR: the internal set of rules outlines the process for making entries in and updating the Registers, and the corporate functions which are from time to time responsible for their keeping. Such corporate functions, each acting within the scope of its competence, are required to fulfil disclosure obligations towards the persons entered in the Registers and Lists and shall comply with any request for access to the Register made by the competent Authorities;
- in addition to the set-up of the Register and Watch Lists, at least the following protective measures are taken for information that directly concerns the Bank. This list is non-exhaustive:
  - when a Register or watch list is set up, the Structure that owns the information (SOP) allocates a code that must be used in the header and text of subsequent communications discussing the topic, as a form of encrypted identification;
  - no specific relevant information may be sent to the SOP team except where this is authorised in advanced by the Manager of the SOP who intends to send the information;
  - the possibility of accessing specific relevant information or inside information must be limited to anyone who needs the information to perform their work, and they must be instantly entered on the watch list or register;
  - when specific significant disclosure is included in shared archives (e.g. email or one drive archives), encryption with a password must be used, where possible;

  - in any case, anyone who has free access to the specific relevant information must be entered, without any further prior authorisation;
  - each member of the Structure who obtains specific relevant information or inside information accidentally, during the course of their work, is required to report this immediately to the Manager of the SOP involved who, based on the available information, will promptly register the incident and will check the robustness of the control measures within their department;
- implementation of best practice logical and physical security systems and other relevant procedures so as to ensure sound management of the information;
- adoption of functional and logistical separation measures (so-called Chinese Walls or Information Barriers) between the organizational structures that provide corporate finance services and activities to customer segments referable to the so-called Corporate side and those that provide investment services and activities or some ancillary services for investors or financial markets referable to the so-called Market side (including treasury, proprietary trading and distribution, through contacts with investors, of the issues made by the Bank for collection purposes) or so-called Research (meaning the Bank Structures responsible for preparing studies and research on investments), so that:
  - no inside or confidential information held by the Corporate side is disclosed to Market side structures;
  - Market-side structures do not report, hierarchically, to the Corporate side structures and cannot be apprised of the other side's transactions or activities, thus ensuring that the two sides operate independently and without influencing each other;
  - the Corporate-side structures in no way influence the Market-side structures in their activities, nor the research and study structures (the same prohibition also applies to the Market-side structures);
  - the structures tasked with preparing studies and researches are kept separate from both Corporate-side and Market-side structures;
- Watch list and Restricted list procedures are put in place, aimed at the management and monitoring of the circulation of insider and confidential information, and at the monitoring of "sensitive" situations (Watch List) that could give rise to conflicts of interest between the Bank and its customers or the market in general or among customers, and at the imposition of further restrictions (Restricted List);
- provision of the obligation incumbent on the employees of the business Structures to provide immediate notification to their manager and to the Compliance department of the occurrence, with regards to a specific transaction that may present the requirements of a sensitive situation falling within the scope of situations of conflict of interest's Watch List (even if only potential), on their own behalf or on that of third parties, especially arising from kinship or spouse relations or from one's own economic or asset interests or those of one's own relative: this without prejudice to the general obligation of abstention provided for by Article 3 of the Group's Internal Code of Conduct;
- provision of rules identifying the fulfilments and limitations to which the members of the corporate bodies, employees and collaborators are subject when they wish to carry out investment transactions on financial instruments on a personal basis: the said rules provide, together with the general prohibitions applicable to all the aforesaid subjects, specific prohibitions and restrictions

for employees and collaborators operating in organisational Structures / Units where there is a greater amount of inside information, as well as reporting, registration and monitoring obligations of the personal transactions permitted;

- procedural and organisational measures are implemented to prevent market abuse offences;
- compliance clearing activities are carried out by the competent Bank Structures, on the information concerning products distributed by the Bank and advertising messages;
- Dedicated Structures are put in place for supervising communication and external relations activities.

All such measures are defined and regulated in greater detail in the internal guidelines, rules and regulations in force from time to time which form an integral and substantial part of this protocol.

The process of disclosing inside information to the market includes the following steps:

- in the case of "price-sensitive" events which are subject to the decision of the Board of Directors, all related communications to the market must be approved by the Board or on the authority of the Board;
- in all other price-sensitive circumstances, the press release will be approved by the Managing Director and CEO, who will inform the Chair of the Board of Directors;
- if the communications directly concern the Bank's and the Group's economic and financial reporting information, the Manager responsible for preparing the financial reports shall issue the attestation provided for by Article 154-bis of the Consolidated Law on Finance;
- if the price-sensitive information relates to circumstances that fall within the sphere of activity of the subsidiaries, the Chair of the Board of Directors, the Managing Directors and/or the General Management of each Subsidiary are responsible for identifying and reporting these, and must promptly contact the Inside Information Management team to ensure that the public disclosure obligations are fulfilled;
- the Co-Head of the Financial Market Coverage team, acting for the Parent Company Inside Information Management Team, who is responsible for the Investor Relations, Price-Sensitive Communication and Financial Analysis & Market Monitoring teams, will prepare the press releases for price-sensitive information for the Group. These releases will be given by Price-Sensitive Communications - after authorisation by the relevant corporate departments - to the competent Regulators via eMarket SDIR. Price-Sensitive Communications will also publish the press releases on the Company's website;
- if the information is only price sensitive for the subsidiaries, or if it relates to circumstances that fall within the sphere of activity of the Subsidiaries issuing financial instruments who are subject to the MAR regulation and which have or may have significant effects on them but not on the Group as a whole, the press releases will be done by the teams and corporate bodies from each of the subsidiaries concerned. They will also - with the written authorisation of Parent Company Inside Information Management and Media and Public Associations Relations - circulate the press releases and publish them on their websites. If the communications directly concern the Bank's and the Group's economic and financial reporting information, the Manager responsible for

preparing the financial reports shall issue the attestation provided for by Article 154-bis of the Consolidated Law on Finance;

- the Co-Head of the Financial Market Coverage team in charge of the Investor Relations, Price-Sensitive Communication and Financial Analysis & Market Monitoring teams is responsible for managing relations with the financial analysts and institutional investors, jointly with the Co-Head of the Financial Market Coverage team in charge of the Rating Agencies Relations and Investor Coverage & Roadshow teams, for the purpose of disclosing relevant information and ensuring its cohesion even if its external publication takes place via the internet;
- the Co-Head of the Financial Market Coverage team in charge of the Rating Agencies Relations and Investor Coverage & Roadshow teams is responsible for managing relations with the rating agencies, jointly with the Co-Head of the Financial Market Coverage team who is in charge of the Investor Relations, Price-Sensitive Communication and Financial Analysis & Market Monitoring teams, for the purpose of disclosing relevant information.

Rules of Conduct

The Corporate Structures, as well as each employee or collaborator, which are howsoever involved in management and disclosure of privileged information shall comply with the procedures set out in this protocol, the applicable provisions of law, the internal rules and any provisions of the Group's Code of Ethics and Internal Code of Conduct.

Specifically:

- all the information and documents acquired in the course of discharging one's duties, whether they concern the Bank or other Group Companies and their financial instruments or third-party Companies having business relations with the Bank and their financial instruments shall be kept confidential; all such information or documents shall be used exclusively in discharge of work-associated duties;
- it is forbidden to carry out transactions on financial instruments of the Bank, Group companies and third-party companies in business relations with the Bank itself, in relation to which the Bank Structures, which order or carry out the transactions, have inside information about the issuer or the security itself, knowing or being able to know on the basis of ordinary diligence the privileged nature of the information, where separation measures (Chinese Wall) envisaged for this purpose were not sufficient to prevent the circulation of the information itself or specific restrictions were arranged. This prohibition applies to any type of transaction in financial instruments (for example: shares, bonds, warrants, covered warrants, options, futures);
- no staff member may perform transactions in advance of customer transactions on the same instruments, since for the purposes of these rules, information on customer orders still to be executed is classified as inside information. This provision also implies the prohibition of transmitting to third parties any information on orders or on information received from the customers;

- inside information may be disclosed within the Bank's Structures only to those staff members who need knowledge of it in order to perform their normal duties and in compliance with existing segregation rules, highlighting the confidential nature of the information and reporting disclosure for the purpose of entering the names of the persons receiving it in the Register of the persons having access to inside information. Furthermore, in the event that a person entered in the Register involuntarily discloses inside information to another person who is not authorised to access it, the person who inadvertently made the disclosure must report the event to the Structure managing the Register for the necessary action;
- it is forbidden to disclose inside information to third parties for any reasons other than performance of duties (for example and without limitation: customers, issuers of publicly-negotiated securities etc.) and in any case where they are not bound to comply with a documentable obligation of legal, regulatory, statutory or contractual non-disclosure, as they are required to arrange for the immediate signing of specific non-disclosure agreements, with particular regard to the relations with counterparties. In any case, the selective disclosure to third parties of the specific relevant information and inside information is only permitted if all the necessary precautions and measures have been taken to avoid its improper internal or external disclosure. The obligation to register all subjects, individually and even if belonging to the same Company, in the Monitoring Lists or in the Register remains valid;
- it is prohibited to advise or induce third parties to carry out transactions linked to the inside information;
- it is forbidden to discuss inside information in public places or in premises where persons not belonging to the company are present or in any case in the presence of persons who do not need to know such information. For example: no inside information can be discussed in open spaces with various facilities, lifts, hallways, snack areas, company canteens, restaurants, trains, airplanes, airports, buses and, in general, places accessible to the general public; special attention must be paid when using cell phones and loudspeaker phones;
- without prejudice to provisions on disclosure to the public of inside information concerning the Bank, it is forbidden to disclose to the market or the media inside information concerning the Bank's corporate customers. If comments on specific transactions concerning such issuers are requested, any comments made shall refer only to facts already disclosed by the issuer under Article 114 of the Finance Consolidation Act; in any case, the bank staff member concerned has an obligation to consult with the corporate functions that lawfully hold the inside information to enable them to check whether confidential information has also been inadvertently disclosed;
- it is forbidden to disclose, either to other staff members or to third parties not belonging to the Bank, through any medium, including the internet, any inaccurate information, rumours or news or information whose accuracy has not been established, and which are likely, even merely potentially, to provide false or misleading information on the Bank or the Group and/or on their financial instruments or on third-party Companies which have business relations with the Bank or the Group and their financial instruments;
- it is forbidden to produce and disseminate studies and researches or other marketing communications in infringement of the internal and external rules specifically laid down for such activity and, in particular, without ensuring that the information provided is clear, accurate and not

misleading, without disclosing in the manner required by law the existence of any significant interests and/or conflicts of interest. It is also mandatory to prepare all documents containing assessments such as the fairness opinion, public recommendation and formal valuation, on the basis of objective elements (financial statements, market practices, financial models, etc.);

- in accordance with the provisions of the internal rules on physical and logistical security all documents containing confidential and reserved information must be filed securely: to this end, staff members shall take care to maintain their own personal password secret and shall ensure that their computer is adequately protected, and that access to it is temporarily blocked wherever they move away from their workstation. Also note that:
  - the production of any documents containing inside information (for example, printing or photocopying of such documents) must be handled by duly authorised staff;
  - the documents in question shall be classified as “confidential”, “reserved” or, where possible, using code names to safeguard the kind of information they contain; when confidential and reserved information is prepared/processed/transmitted/filed in electronic format access to such information shall be password protected or, for those Structures so equipped, will involve the use of encryption software;
  - the physical supports containing confidential and reserved information must be kept in secure controlled-access premises, or placed in controlled or protected archives after their use, and must never be left unattended, especially when they are taken outside the workplace;
  - destruction of the physical supports containing confidential and reserved information must be carried out by the same persons responsible for them, using appropriate procedures to avoid any unauthorised retrieval of the information they contain.

Furthermore:

- with particular regard to the issue of official communications to the market, such communications shall be prepared in compliance with the applicable laws and regulations and, in any case, fully respecting the requirements of correctness, clarity, and equal access to the information, where:
  - correctness means exhaustive and non-misleading information, having regard to the legitimate requests for data and news coming from the market;
  - clarity refers to the forms in which the information is communicated to the market and means that it must be complete and clearly understandable, also taking into account the intended recipients of the communications;
  - equal access means that no information that might be relevant for assessment of financial instruments may be communicated in any manner that is howsoever selective. The case in point also includes the unintentional dissemination of privileged information for which company regulations anticipate an immediate notification of the event to the competent function to allow the timely dissemination of the press release in accordance with the procedure relative to communicating price sensitive information to the market;
- the disclosure of inside information to the Supervisory Authorities shall take place in an exhaustive, timely and appropriate manner, in compliance with the applicable rules and regulations. Prior to this communication no declaration concerning inside information may be released to external parties.

Lastly, the Bank has adopted an “Internal dealing” regulation which sets out specific rules of conduct based on the legal reporting requirements for transactions performed on the financial instruments of a listed issuer by relevant and/or related parties, pursuant to Article 19 of the MAR and to the Issuers’ Regulation (Consob resolution 11971/1999 as subsequently amended and supplemented) for the purpose of ensuring that the information provided to the market meets the highest standards of transparency.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.8.2.2. Managing orders and market transactions to prevent administrative and criminal offences linked to market abuse

Introduction

This protocol applies to all the Bank Structures involved in the management of market transactions on financial instruments.

The process of managing market transactions presents potential opportunities for commission of the offences of market rigging and market manipulation or the corresponding administrative breach, covered respectively by Article 2637 of the Civil Code, and by Articles 185 and 187-*ter* of the Consolidated Law on Finance, with reference to the conduct of "operating manipulation" described by those provisions.
As regards the prevention of crimes and administrative offences concerning the "manipulation of information" - which may involve disseminating information, rumours or news that are false or misleading - reference is made to the protocol in paragraph 7.7.2.1, on the "*Management and disclosure of information for the prevention of crimes and administrative offences concerning Market abuse*", which sets out the principles of control and conduct to observe in the process to manage the inside information that could come to the knowledge of the Bank's operating structures in performing assigned duties, or in relation to the Bank's communications to the market, and in general, to external sources.

The purpose of the rules set out in this document, in accordance with the requirements of current legislation, is to ensure that during execution of trading and settlement transactions on the market – or when orders to execute such transactions are given to third parties - no simulated transactions or other fictitious devices likely to have a significant effect on the prices of financial instruments are carried out, or transactions or other fictitious devices likely to provide false and misleading information on the offer, demand for, or the price of the financial instruments.

The definitions given in this protocol are aimed at ensuring the Bank's compliance with applicable regulations and principles of transparency, correctness, objectivity and traceability in carrying out the activities concerned.

Process description

The process of managing orders and market operations, for the purposes of this protocol, concerns trading activities, both on own account and for third parties, concerning the financial instruments

referred to in Article 182 of the TUF and executed directly by the Bank or through third parties (in particular brokers) to whom orders for their execution are forwarded.

As to trading on the Bank's own behalf, the process comprises the following main activities:

- defining the general guidelines for managing the portfolio of securities owned by the Bank;
- planning investment strategies on the basis of the analyses and proposals submitted to the approval of the competent Bank bodies or structures;
- management of the portfolio and/or of ownership risk (VAR) and performance trading activity, arbitrage and the taking of long/short positions on cash products and derivatives, taking positions exposed to interest rate risk, exchange rate risk, credit risk, equity risk and volatility risk, in compliance with the notional limits, VAR limits and the limits of the expected risk/return profile;
- management of the portfolio of investments in alternative funds, traditional funds and related instruments;
- support to intermediation in the Bank's own bonds;
- technical support to the management of financial profiles of the Bank's investments in listed stocks;
- management of trading in own shares on the markets;
- direct or indirect execution on the markets of trading transactions for managing the Bank's security portfolios;
- fulfilment of the administrative/regulatory requirements associated with performance of the trading transactions.

With regard to the Bank's trading activity on behalf of third parties (executing orders on behalf of customers and receiving/transmitting orders) or to trading on own account (also if finalised directly with customers), an automatic procedure is in place which selects and monitors suspicious transactions which are subsequently analysed for the purposes of preventing crimes or administrative offences concerning market abuse. If at the time of receiving an order there are reasons to believe or suspect that execution of the transaction is instrumental to the commission of an offence or an administrative breach or to obtaining the proceeds of such offence or breach, the operator should consider whether the transaction should be denied or suspended.

The operating methods for managing the process are governed as part of internal regulations developed and updated by the competent Structures, which constitute an integral and substantial part of this protocol.

Control principles

The system of controls for monitoring the process described is based on the following factors:

- Authorization levels defined on the basis of the current system of powers and proxies approved by the Board of Directors:
  - the guidelines for the management of the Bank's portfolio of current and non-current securities;
  - the operating perimeter for trading financial instruments on the market;
  - decisions authorising the performance of equity investments/divestments;
  - operational limits according to the role covered and/or the position of the personnel concerned;
  - the structuring of transactions connected with the provision of investment and ancillary services and market transactions.

- Organisational separation (Chinese Walls) between the Structures which deal with inside information (in particular between those that manage business relations with the corporate customers, grant and manage credit, provide corporate finance services, and manage subsidiaries and equity investments) and those which hold direct relations with the market, including the structures engaged in the production of studies and researches on issuers of listed financial instruments and those performing trading activities (on behalf of the Bank or of third parties, including asset management) and sales activities.

- Participation of several subjects, belonging to the same Organizational Unit and to several Organizational Units in the structuring of transactions related to the provision of investment services, accessories and market transactions.

- Control activity on purchase and sale transactions executed on the markets by means of a differentiated control system which takes into account the different types of financial instruments dealt with and the specific features of the reference market.

- Existence of specific Committees, as indicated in internal regulations that carry out risk controls at the level of the structure and of third-party counterparties involved in the transactions, also authorizing entry on new markets or the introduction of new products, subject to the involvement, where required, of the Committee Evaluating Impacts of New Products/Services.

- Monitoring of investment service activities by second level control functions of the Bank, in particular the Compliance function which, for the aspects falling under its competence, performs prior validation activity and ongoing monitoring of the appropriateness of the internal procedures concerning the provision of investment services, including verification of compliance with reference legislation, taking into account the findings of the Internal Auditing Function.

- Process traceability including both the electronic and the paper trail: in particular, financial instrument purchase and sale transactions are managed through dedicated software systems, where all details of the transactions executed are saved.

- The general principles covering operations management are set out in the detailed internal rules which address, in particular, the following aspects:
  - identification of the intermediaries authorised to operate with the Bank, trading and conclusion procedures (quotation and execution), trading times, late deals, “fast” payments relating to OTC derivative transactions, processes for the authorisation of new products, access to trading rooms, authorised traders, errors, litigations and complaints.

Rules of Conduct

The Bank’s structures howsoever involved in the management of customers’ assets or in trading activities, on the Bank’s behalf or on account of third parties, through negotiation and settlement of transactions on the markets, shall comply with the procedures set out in this protocol, the applicable provisions of law, the internal rules and any applicable provisions of the Group's Code of Ethics and Internal Code of Conduct.

In particular it is forbidden to:

- set up sham transactions or employ other fictitious devices likely to significantly affect the price of financial instruments;
- undertake transactions or issue purchase or sale orders which provide or are likely to provide false or misleading indications on the offer, demand for or price of financial instruments;
- undertake transactions or purchase and sale orders making it possible, also through the coordinated action of several persons, to fix the market price of financial instruments at an abnormal or artificial level;
- undertake transactions or purchase and sale orders employing fictitious devices or any other form of deception or contrivance;
- use other fictitious devices likely to provide false or misleading indications on the offer, demand for or price of financial instruments.

The following types of conduct concerning the financial instruments referred to in Article 182 of the Finance Consolidation Act are forbidden, with the exception of those cases and procedures set out in current legislation:

- undertake transactions or give orders to trade which represent a significant proportion of the daily volume of transaction in the relevant financial instrument on the market concerned, in particular when these orders or transactions lead to a significant change in the price of the financial instrument;
- undertake transactions or give orders to trade when holding a significant buying or selling position in a financial instrument leading to significant changes in the price of the financial instrument or related derivative or underlying asset;

- undertake transactions leading to no change in beneficial ownership of the financial instrument;
- undertake transactions or give orders to trade which include position reversals in a short period and represent a significant proportion of the daily volume of transactions in the relevant financial instrument on the market concerned, and might be associated with significant changes in the price of a financial instrument;
- undertake transactions or give orders to trade which are concentrated within a short time span in the trading session and lead to a price change which is subsequently reversed;
- give orders to trade that change the representation of the best bid or offer prices in a financial instrument, or more generally change the representation of the order book available to market participants, and are removed before they are executed;
- undertake transactions or give orders to trade at or around a specific time when opening or closing auction prices, control prices, reference prices, settlement prices and valuations of financial instruments are calculated and lead to price changes which have an effect on such prices;
- undertake transactions or give orders to trade which are preceded or followed by the dissemination of false or misleading information, by persons or persons related to them that have given orders or traded;
- undertake transactions or give orders to trade before or after producing or disseminating research or investment recommendations which are erroneous or biased or demonstrably influenced by material interest.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.9 Sensitive area concerning workplace health and safety offences

*7.9.*1 Types of offences

Introduction

Article 25-*septies* of the Decree includes in the list of the predicate offences giving rise to the liability of Entities the offences of unintentional killing (manslaughter) and of unintentionally causing grievous bodily injury where such offences are committed through violation of accident prevention and workplace health and safety rules.

The Consolidated Law on protection of health and safety in the workplace (Legislative Decree 81 of 9 April 2008), reorganised in a coherent framework the large number of previous legislative acts governing this area, with Article 30 setting out the required contents of the Organisational, Management and Control Model in this area for the purpose of preventing the offences in question.

The purpose of the above legal provisions is to provide more effective means of prevention and punishment, in the light of the spike in the number of workplace accidents and of the need to safeguard the physical and mental wellbeing of workers and the safety of workplaces.

The above-mentioned offences are briefly described below.

Involuntary manslaughter (Article 589 of the Criminal Code)

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

The two offences consist in culpably causing respectively death or serious or grievous bodily harm.

Serious bodily injury indicates a condition which endangers the life of the injured person, or causes incapacity to attend to normal activities for a period exceeding forty days, or an injury which results in the permanent weakening of a sense or an organ; grievous bodily injury indicates a probably incurable condition; the loss of a sense, a limb, an organ or the capacity to procreate, permanent impairment of the power of speech, and facial deformity or permanent disfigurement.

Under the above-mentioned Article 25 *septies* of the Decree, to give rise to the Entity's liability, both conducts must be characterised by violation of workplace accident prevention and health and safety protection regulations.

Various legal provisions cover this area, most of which have been since absorbed by the Consolidated Law on the protection of workplace health and safety, which repealed many of the previous special laws, among which we should mention: Presidential Decree 547 of 27.4.1955 on accident prevention; Presidential Decree 303 of 19.3.1956 on workplace hygiene; Legislative Decree 626 of 19.9.1994 which contained general provisions on the protection of workers' health and safety; and Legislative Decree 494 of 14.8.1996 on construction site safety.

The specific prevention requirements set out in sector legislation are complemented by the more general provision of Article 2087 of the Civil code, which requires employers to set in place measures

to protect the physical and mental health of workers having regard to the characteristics of the work, the workers' experience and the techniques employed.
Lastly, it should be noted that according to case law the employer may also be liable for the offences in question where the injured person is not a worker but a third party, provided that his presence at the workplace at the time of the accident was neither anomalous nor exceptional.

7.9.2 Sensitive company activities

The protection of occupational health and safety is a requirement applying throughout all companies, areas and activities.
We reproduce below the protocol laying down the control principles and rules of conduct applicable to the management of the risks relating to workplace health and safety. This protocol is completed by the applicable detailed corporate regulations in force.

Such protocols also apply to the monitoring of any activities performed by Group companies and/or outsourcers on the basis of special service agreements.

7.9.2.1. Management of the risks relating to workplace health and safety

Introduction

The management of the risks relating to workplace health and safety concerns any type of activity aimed at developing and putting in place a system for the prevention of and protection against workplace risks, in accordance with the contents of Legislative Decree 81/2008 (hereinafter, the Consolidated Law).

First of all, it is worth recalling that pursuant to the Consolidated Law, the Employer has a duty to establish a company policy addressing workplace health, while the Principal and/or his delegates are responsible for and manage the temporary or mobile worksites governed by Title IV of the Consolidated Law, and both, within the scope of their respective competences, must fulfil the obligations relating to the award of supply/works contracts set out in Article 26 of the same Consolidated Law.

In accordance with the provisions of such Law, the Bank has adopted and keeps updated a "Risk Assessment Document", containing:

- assessment of the health and safety risks to which workers are exposed in the course of their work activity;
- identification of the prevention and protection measures adopted to safeguard the workers and of the programme of measures deemed appropriate to upgrade safety levels within the short term;
- identification of the procedures for implementing the measures so identified, and of the corporate structures and officers responsible for them, who shall be solely persons possessing the appropriate competences and powers;
- identification of the Officer Responsible for the Prevention and Protection Service, of the Workers' Safety Representatives and of the Competent Medical Doctors who have participated in the risk assessment;
- identification of the tasks which might expose workers to specific risks requiring proven professional skills, specific experience and appropriate training and updating.

This Document is prepared in compliance with national legislation and national and European guidelines (ISPESL, INAIL, UNI-EN-ISO, European Agency for Safety and Health at Work). More specifically, the UNI-UNAIL "Guidelines for a Health and Safety Management System at Work (SGSL)" were implemented in September 2001. To this end, the Risk Assessment Document identifies, within the corporate organisation, the responsibilities, procedures, processes and resources for the implementation of its own prevention policy in compliance with applicable health and safety regulations. The same Document describes the methods with which the organisation meets the requirements of the aforesaid Guidelines and outlines the operational processes and corporate documents aimed at guaranteeing the fulfilment of the provisions laid down by Article 30 – Organisation and management models – of the Consolidated Law.

The Bank has adopted and maintains an Occupational Health and Safety Management System, which is verified annually by an international Certification Body, conforming to applicable laws and the most up-to-date reference standards: UNI ISO 45001 (in 2018, ISO replaced the British Standard Occupational Health and Safety Assessment Series - OHSAS 18001:2007).
Furthermore, the Bank has chosen to obtain quality certification of the processes managed by the Prevention and Protection function in accordance with UNI EN ISO 9001:2015.
The company has adopted a system of functions appropriate to the nature and size of the organisation and type of activity carried out, ensuring the necessary technical competences and powers for risk verification, assessment, management and control.

The corporate Structures in charge of managing OH&S documentation, including authorisations/certifications/favourable opinions issued by the Public Administration, must comply with the rules of conduct set out and described in the protocol "*Management of activities relating to the request for authorisation or fulfilment of requirements towards the Public Administration*".

The company's workplace health and safety policy must be disseminated, understood, applied and updated throughout the organisation and at all levels. For this purpose adequate training plans are drawn up, complying with applicable regulations, that take into account the company position held, exposure to specific risks and the assignment of particular duties to manage the emergency situation. The Bank's general guidelines must target ongoing improvement of the quality of health and must contribute to the development of an effective "prevention and protection system". All the Bank's structures must comply with the provisions on workplace health, safety and hygiene, and take them into due account whenever changes to the existing organisational setup are introduced, including workplace restorations/setups.

The definitions given in this protocol are aimed at ensuring the Bank's compliance with applicable regulations and principles of transparency, correctness, objectivity and traceability in carrying out the activities concerned.

Process description

The workplace health and safety risk management process comprises the following phases:

- identifying and classifying hazards (including both safety hazards and occupational health hazards);
- carrying out risk assessment;
- defining and developing prevention and protection measures;
- preparing an action plan and allocating actions among the various corporate structures;
- implementing the planned actions in the framework of a programme;

- monitoring implementation and checking the effectiveness of the measures adopted.

With specific reference to construction site management (Articles 88 et seq. of the Consolidated Law) which falls under the responsibility of the "Principal", the process comprises the following phases:

- verifying the technical and professional competence of the contractors/subcontractors and self-employed workers;
- appointment of the Project manager and, where necessary, of the Site engineer, the design Coordinator and the works Coordinator, subject to verification of the professional requirements of the subjects in charge and formalisation in writing of the relevant appointments;
- planning of the works phases and their evaluation with special reference to the interactions of the activities also having an impact on the surroundings of the work site and the possible concurrence of the Bank's activities and preparation of the safety and coordination plans or, where interference risk evaluation documents are not provided for by regulations, also on behalf of appointed professionals;
- preparation of requests for proposals with information to the counterpart as to the arrangements in place on the subject of health and safety (safety and coordination plans/interference risk evaluation documents);
- preparation of the proposal by the offeror with indication of the costs allocated to health and safety relating to the measures in place to manage interferences, on the basis of the scope and characteristics of the service/supply being offered, as well as containing a statement of acknowledgement of the risks present in the places where the work is carried out and of the relevant measures aimed at their elimination/reduction;
- fulfilment of technical-administrative obligations, notifications and communications to the public administration, including on behalf of the professionals in charge;
- awarding of the service and stipulation of the agreement, with the indication of the costs relating to safety and attachment of the safety and coordination plan/interference risk evaluation document;
- coordinating performance of activities by the various contractors/self-employed workers and carrying out site controls in compliance with the required measures, also through the professionals appointed for this purpose.

At temporary or mobile construction sites where Bank employees are present, the risks arising from interference between the two activities are managed by the Principal, even through professionals specifically appointed for this purpose, by identifying the prevention, protection and emergency measures safeguarding the health and safety of the employees, customers, contractors and self-employed workers. Such measures are set out in the Safety and Coordination Plan or, if not provided for therein, in the Single Interference Risk Assessment Document (having regard to their respective scopes) prepared by the persons appointed by the Principal, with support, as required, of the Bank’s Prevention and Protection structure.

With specific reference to the management of supply contracts, works contracts and service contracts falling within the scope of Article 26 of the Consolidated Law the process comprises the following phases:

- verifying the technical and professional competence of the contractors/subcontractors and of the self-employed workers;
- providing information to the subcontractors/self-employed workers on the specific risks at work sites, and on the prevention and emergency measures adopted, having regard to the activities covered by the contract; moreover, where provided for by the law or regulations, preparing the Interference Risk Assessment Document (DUVRI), to be supplied to bidders for the purpose of preparing their bid, and which will constitute an integral part of the contract, containing the appropriate measures for eliminating or reducing the risks arising from the interference of other activities with those required for contract performance, and simultaneous preparation of the request for bids, where provided for;
- preparation of the bid by the bidder, indicating the costs earmarked for safety measures and interference management measures, which shall be proportionate to the scope and characteristics of the supply/works offered, and shall contain a statement to the effect that the bidder has been informed of the risks present at the proposed construction site, together with a description of the proposed measures to eliminate/reduce those risks;
- award and signing of contract, indicating the cost earmarked for safety measures and annexing the DUVRI;
- performance of the supply/works contract by the selected contractor with specific indication of personnel appointed as Officer, cooperation and coordination with the subcontractors/self-employed workers to implement occupational risk protection and prevention actions, also via the exchange of information to eliminate the risks due to any interference between the works of the different contractors involved in performance of the overall project and the risks linked to the concurrent presence of the Bank's agents, employees and customers on site;
- control on compliance with contractual requirements in performance of activities.

The Employer has delegated the Head of the Property function, for the activities falling under its competence, for the purpose of fulfilling the obligations set forth in above mentioned Article 26; such activities can be further delegated to other specifically appointed persons.

With specific reference to health surveillance, the process comprises the following steps:

- identification and appointment of the Competent Doctor;
- performance of health surveillance:
  - annual planning of activities (medical check-up dates expiring, and inspections of work areas) shared with the Competent Doctors;
  - periodic updates during the year and controls to evaluate any need to introduce improvement plans;
- periodic processing of epidemiological reports based on anonymous data related to health surveillance; this activity contributes to evaluating and preventing any negative effect on the health

and welfare of workers and, consequently, also to identifying/evaluating new or unusual risk factors in the work context

The Competent Doctor's inspection of the work place of each operator is strictly related to health surveillance. The aim of the inspection is to enable a complete review of the results of the above activities, provide contextualised opinions on the suitability of the work area and suggest specific, additional analyses based on inspection findings.

With specific reference to the analysis of occupational accidents and diseases, the process comprises the following steps:

- the activation of a preliminary stage to control and further investigate information and documents;
- an inspection, conducted - if necessary, to identify the primary cause of the event;
- the definition of any corrective measures to adopt.

With specific reference to the assessment of work-related stress, the methodological approach selected to assess the risk of work-related stress is based on research of the Occupational Medicine Department of ISPESL[64] and comprises the following steps:

- preliminary assessment (necessary/mandatory);
- in-depth assessment (if any).

The assessment is conducted by a "Team managing the assessment", that plans, coordinates and applies the entire process. The Team comprises – in compliance with the Consolidated Law: i) the Employer (or his/her representatives); ii) Safety Department Manager and Safety Department Operators; iii) Coordinator Doctors and competent Medical Doctors. This Group also consults workers and/or Workers' Safety Representatives (if present) and is assisted by company functions considered necessary in relation to the Company's characteristics (Human Resources, Organisation, Training, Legal Affairs, etc.), and also by external specialist consultants, as applicable.

Lastly, with specific reference to finance leases for real estate and/or moveable property, the Bank checks the conformity of said to occupational health and safety regulations, at the time of purchase and granting to customers, and also at the time of repossession, re-use or resale following the end of leasing for any reason whatsoever.

Procedures to manage and control the process are based on a clear, formalised assignment of duties and responsibilities with reference to the Structures involved (including external outsourcers) in controls on compliance with health and safety regulations in force from time to time, and on a consistent system of authority, that governs the functions and powers arising from the regulatory obligations of the Consolidated Law.

[64] This activity is now overseen by INAIL: "Assessment and management of work-related stress. Manual and use of companies in implementing the Consolidated Law as amended".

The operating procedures for managing the process and identifying the structures/roles in charge of the different phases are governed by internal rules, which are developed and updated by the competent Structures and form an integral and substantive part of this protocol.

Control principles

The control system for monitoring the process described above must be based on the following elements:

- Authorisation levels defined within the process:
  - the company's management system defines specific responsibilities and procedures to allow the full implementation of the workplace health and safety policy with a systematic and planned approach. In particular, the company figures playing respectively the roles of "Employer" and "Principal" must be identified. Such figures are empowered to issue health and safety related instructions to the company's Structures and are endowed with the broadest organisational autonomy and spending powers. They may also delegate and sub-delegate tasks, pursuant to Article 16 paragraph 3-*bis* of the Consolidated Law;
  - a system of different functions is in place, to ensure the necessary technical competences and powers for risk verification, assessment, management and control;
  - all the persons/corporate roles taking part in the phases of the above-mentioned process must be identified and authorised by an express provision of the internal rules or by means of delegation, to be issued and kept on file by the Employer/Principal, or by the persons appointed by them.

- Segregation of the duties between the different persons/corporate roles involved in the Risk Management Process relating to workplace health and safety. Specifically:
  - the operational Structures responsible for implementing and managing projects (real estate, IT, physical security, or relating to work processes and staff management), shall be distinct and separate from the Structure which is appointed under the law and/or the internal rules, to provide advice on risk assessment and on the monitoring of risk prevention and reduction measures;
  - the competent structures shall appoint persons having specific responsibilities for managing/preventing occupational health and safety risks;
  - The workers' safety representatives shall actively collaborate with the Employer, reporting any problems identified and helping to pinpoint appropriate solutions.

- Control activities:
  - the competent structures must put in place a corporate plan of systematic controls ensuring periodic assessment of the sound application/management and of the effectiveness of the

occupational health and safety procedures in place and of those measures implemented to assess workplaces in accordance with the requirements of law. In particular, the plan shall cover:

- corporate areas and activities to be assessed (including organisational activities[65], health surveillance, worker information and training, and monitoring of workers' compliance with health and safety requirements in performance of their duties);
- procedures for performing verifications, reporting procedures.

The company plan must also ensure:

- compliance with the technical-structural standards required by law in respect of equipment, plant, workplaces, and chemical, physical and biological hazards;
- provisions to ensure that the competent structures obtain the documentation and certifications required by law (concerning buildings, (concerning buildings, plant, positions, appointments, qualifications, personnel and companies etc.);compliance with the process and technical and administrative requirements set out in the internal regulations and applicable laws.

An appropriate control system shall also be put in place with regard to the effective implementation and ongoing maintenance of the conditions of appropriateness of the measures adopted. The plan shall be reviewed and amended in an appropriate manner whenever significant infringements are detected to the rules on accident prevention and workplace hygiene or whenever organisational and operational changes are made to incorporate scientific and technological developments;

- the competent Structures shall ensure that all the planned prevention and protection measures are implemented, providing ongoing monitoring of risk situations and of the progress of the action plans established by the specific risk assessment documents. Such Structures shall avail themselves as appropriate of the cooperation of the Structure responsible for managing human resources, and of the structures in charge of managing and implementing real estate projects, workflow design and management processes, physical security, information systems, management and maintenance, the assignment and management of leased real estate and moveable property;
- the Workers' Safety Representatives, acting in compliance with applicable legislation, are entitled to access the company's documents relating to risk assessment and associated prevention measures and to request additional information on the subject. These Representatives shall also be authorised to access workplaces and make observations at the time of inspections and checks by the competent Authorities;
- all workplaces shall be visited and assessed by persons meeting the legal requirements and having appropriate technical qualifications. The Competent Doctor Officer in charge and staff of the Prevention and Protection Service shall visit the workplaces where workers are exposed to specific risks and shall carry out spot checks in the other workplaces;

[65] Including emergencies, first aid, supply/works contract management, regular safety meetings, consultations with the workers' safety representatives

- specialist figures possessing proven professional expertise and meeting the requirements provided for by specific standards assessed on a prior basis, shall contribute to the assessment process and to planning protection measures in respect of specific risks, specifically:
  - the Competent Coordinator Doctor: appointed by the Employer, guarantees health surveillance obligations of regulations, assists the Employer and the Safety Department in assessing risks, preparing and adopting measures to protect workers' health and mental wellbeing; combines and updates, after notifying the Local Competent Doctors, the health surveillance protocols with related documentation and procedures;
  - The Local Competent Doctor: appointed by the Employer, for areas in its remit, plans and conducts health surveillance based on the health protocols defined considering specific risks using the general guidelines provided by the Competent Coordinator Doctor and the Risk Assessment Document, and gives an opinion on fitness for the specific task, notifying the outcome in writing to the Employer and worker;
  - the Person in Charge of Asbestos Risk: is appointed based on point 4 of Ministerial Decree DM 06/09/94 and is "tasked with controlling and coordinating all maintenance activities that may involve materials in asbestos", complying with safety measures (for cleaning, maintenance and for each event that may cause a disturbance to MCA), providing the occupants of the building with correct information on the presence of asbestos, potential risks and the conduct to adopt;
  - the Radiation Protection Expert: is appointed by the Employer, and conducts analyses and necessary assessments for the purposes of the physical surveillance of the protection of individuals of the population;
  - the Expert qualified to manage radon clean-up activities: provides technical indications in order to adopt corrective measures to reduce the concentration of radon in buildings pursuant to Article 15 of Legislative Decree 101/10;
  - the fire-fighting Professional: prepares preventive opinions, applications for the assessment of projects, certifications and statements on construction elements, products, materials, equipment, devices and plants which are relevant for fire safety purposes; and as regards work sites (Title IV of the Consolidated Law):
  - the Project Manager: is appointed by the Principal to carry out the duties assigned under Article 90. He/she takes on all powers and responsibilities of legal obligations to supervise the work site, also guaranteeing compliance with all safety regulations in applicable provisions;
  - the Planning Coordinator: is appointed by the Principal or Manager in cases required by law. He/she is in charge of drafting the Security and Coordination Plan (PSC);
  - the Works Coordinator: is required to carry out coordination at the work site and also control work procedures. The duties of the Works Coordinator include, among others, the "validation" of the operational safety plan, controls, with appropriate coordination and control actions, of companies performing works, independent workers, complying with the provisions applicable to them in the PSC and the correct adoption of work procedures. This Coordinator also suspends works in the event of a serious, imminent danger.

- the competent Structures identified by the Employer/Principal shall also assess the technical and professional competence of contractors or self-employed workers in respect of the tasks assigned to them;
- the competent Structures identified by the Principal shall assess the technical and professional competence of the Project supervisors, the Site engineer, and the works Coordinator in relation to the specific characteristics of the works to be executed under the works contracts.
- if the documentation required under the Consolidated Law is maintained on electronic medium, the competent Structure shall check that the data saving methods and the procedures for accessing the data management system are in compliance with Article 53 of the Consolidated Law;
- the Employer and the Principal, each within their respective spheres of competence, acting in accordance with paragraph 3-*bis* of Article 18 of the Consolidated Law, shall supervise the compliance of agents, workers, competent doctors, designers, manufacturers, suppliers, and installers with their obligations under health and safety legislation through the above-mentioned company-wide systematic control plan.
- With regard to temporary or mobile worksites, the Principal verifies that tasks are correctly assigned and that the Site engineer, the Project manager, the design Coordinator and the works Coordinator, where appointed, duly fulfil their obligations and that the contractor's officer has been named; for this purpose, the Principal receives from them periodic reports on the activities carried out, critical issues, if any, and the measures adopted to rectify them;
- the competent structures delegated and/or identified by the Employer and Principal must check:
  - that the real estate and/or movable property to purchase to assign through finance leases are in conditions that ensure they conform to applicable regulations, checking that required conformity statements and documentation required by law have been provided;
  - that in cases of the repossession of real estate and/or moveable property, or where information is obtained concerning possible user violations of health and safety regulations, all related actions, also of a legal nature, functional to managing occupational health and safety risks, are carried out diligently and in adequate times;
  - that the repossessed real estate and/or moveable property have been assessed for exposure to occupational health and safety risks, and actions to make them safe have been planned.
- the competent Structures identified by the Employer, check that the qualifications and requirements of the Competent Doctors and specialists that are involved in individual processes are maintained over time;
- the Officer notifies the competent Structures identified by the Employer of any delay in complying with the provisions of the Competent Doctor, in order to activate necessary measures;
- the competent Structures identified by the Employer, periodically check the correct management of preliminary investigations into occupational accidents.

- Process traceability including both the electronic and the paper trail:

- the use of systems for the electronic management of data and documentation required by the Consolidated Act must comply with Article 53 of said;
- in order to allow reconstruction of responsibilities, each Structure from time to time concerned shall put in place adequate systems for recording activities performed, and shall be responsible for filing and storing, also in telematic or electronic format, all executed contracts and all the documentation produced as part of its activities relating to management of workplace health and safety risks and the associated control activity;
- each Structure from time to time concerned shall also be responsible for acquiring, storing and filing the documents and certifications required by law, as well as any documentary evidence of the technical and professional expertise of contractors, self-employed workers and persons appointed as responsible for workplace safety (e.g. the Project manager, design and works Coordinators);
- management of the different risk contexts provides for the use of specific information systems accessible via the intranet by all the Structures concerned and authorised to carry out risk assessments relating to the operating units. These information systems shall contain, for example, the technical documentation of plant, machinery, workplaces, etc., the lists of employees exposed to specific risks, the health documents (in compliance with the confidentiality requirements provided for by legislation), training and information activities, risk elimination/reduction activity, internal and external inspections, information on injuries and risk reporting, forms for the management of environmental monitoring and health records, etc..

Rules of Conduct

The Bank Structures howsoever involved in the management of the risks relating to workplace health and safety, as well as all employees shall comply with the procedures set out in this protocol, the applicable provisions of law, internal rules and any provisions of the Group's Code of Ethics and Internal Code of Conduct.

In particular, all the Structures/roles are obligated – within their respective spheres of competence - to:

- ensure, within their sphere of competence, performance of the measures relating to occupational health and safety, by implementing general protection measures and assessing the choice of work equipment and workplace layout and organisation;
- request the issue of declarations of conformity of owners, required by law, for the leased real estate and/or moveable property;
- if third parties are to be involved in the management/prevention of workplace health and safety risks, the contracts entered into with such persons shall contain a specific declaration that they are aware of the provisions of Legislative Decree 231/2001 and undertake to comply with them;
- avoid appointments of external consultants that are not made on substantiated and objective grounds of professionalism and expertise, competitiveness, price, integrity and the ability to provide effective assistance. In particular, the rules for the selection of professionals shall refer to the criteria of clarity and availability laid down in the Group’s Code of Ethics and Internal Code of Conduct;

- adopt transparent and cooperative conduct towards the Agencies in charge of performing controls (e.g. Labour Inspectorate, Local Health Authorities, the Fire-fighting agencies, etc.) when such agencies carry out checks or inspections;
- when awarding supply/works contracts, inform the contractors of the specific risks present at the worksites where they will operate, and apply measures to ensure the safe management of any interferences between contractors, including any self-employed workers, highlighting the planned cost of safety measures in the contracts where such indication is provided for;
- foster and promote internal information and training on work-related risks, on the prevention and protection measures and activities adopted, first aid procedures, fire-fighting measures and worker evacuation procedures;
- ensure compliance with the health and safety rules and legislation by all workers who are not Bank employees, with particular reference to the contracts governed by Legislative Decree 81/2015 as subsequently amended and supplemented, to individuals operating under training schemes and to any third parties who might be present in the workplaces;
- ensure that, in respect of automatic data processing systems, data saving methods and the procedures for accessing the required documentation management system meet the requirements set out in Article 53 of the Consolidated Law.

Likewise all employees shall:

- Comply with legal provisions and internal regulations and directives given by the company's Structures and the competent Authorities;
- use in an appropriate manner machinery, equipment, tools, means of transport and all other work equipment, and safety devices;
- report immediately to the officer in charge of emergencies or his subordinates any potential or real danger situation and, in case of emergencies, take all steps within their competences and possibilities, to eliminate or reduce the hazardous situation.

In any case, it is forbidden to engage/collaborate in or induce conduct (or omissions) which may belong to one of the types of offences covered by Legislative Decree 231/2001. In particular, as regards real estate and/or moveable property leased through finance leases, it is forbidden to:

- authorise the purchase, or in any case authorise the financial leasing of assets that do not conform to legal provisions and regulations in force;
- authorise the sale or a new lease for real estate and/or moveable property through finance leases that do not conform to legal provisions and regulations in force, save for any exceptions limited to cases where the asset is sold to a professional (supplier with proven knowledge and experience, authorised dealer, etc.), relieving Intesa Sanpaolo S.p.A. of all legal liability.The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.10 Sensitive area concerning computer crimes and the unlawful use of non-cash payment instruments

7.10.1 Types of Offences

Section I – Computer crimes

Introduction

Law No 48 of 18.3.2008 ratified the Convention on Cybercrime of the Council of Europe, signed in Budapest on 23.11.2001, aimed at fostering international cooperation between the States parties to the Convention in order to combat the spread of cybercrime directed against the confidentiality, integrity and availability of computer systems, network and data, especially in consideration of the nature of such crimes, whose planning or commission often involve different countries.

The reform of the legislation on cybercrime was carried out both by introducing new types of crimes in the Criminal Code and by amending certain existing crimes. Article 7 of the Law has also added to Legislative Decree 231/2001 Article 24-*bis*, which lists the series of computer crimes which might give rise to the administrative liability of Entities.

The above-mentioned law has also amended the Code of Criminal Procedure and the provisions relating to the protection of personal data, essentially in order to facilitate investigations of computer data and allow for the preservation of internet traffic data for certain periods.

On the other hand, the Italian legal system has not implemented the definitions of "computer system" and "computer data" provided by the Budapest Convention; such definitions, which are reproduced hereunder, may however be taken as a reference by case law in this area:

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

The predicate offences listed by Article 24-*bis* of Legislative Decree 231/2001 are described below.

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

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

For the offence to occur it is not necessary that it be committed for the purpose of making a profit or damaging the system; the offence occurs also where the purpose is to demonstrate the hacker's

ability and the vulnerability of the system; however, unauthorised access is in most cases aimed at damaging the system or perpetrating frauds or committing other computer crimes.

The offence is prosecutable on the action of the injured party; however, it is prosecutable ex officio where the specific aggravating circumstances set out in the Article are present, including: if the deed causes the destruction or the damage of the data, the software or the system or the partial or total interruption of its operation; if the deed concerns systems of public interest; or if the deed was committed by abusing one's role as system operator.

In the corporate context, the offence may also be committed by any employee who, while possessing system access credentials, accesses parts of the system which are off limits to him, or accesses, without authorisation a database of the Bank (or also of third parties which the Bank is licensed to use), by using the credentials of other, authorised, co-workers.

Wiretapping, blocking or illegally interrupting computer or information technology communications (Article 617-*quater* of the Criminal Code)

Unauthorized possession, distribution and installation of devices and other equipment for wiretapping, blocking or interrupting computer or information technologies communications (Article 617-*quinquies* of the Criminal Code)

The conduct punished by Article 617-*quater* of the Criminal Code consists in fraudulently wiretapping communications within a computer system or telecommunication system or between several systems, or blocking or interrupting such communications. The same offence is committed, unless the deed constitutes a more serious offence, when the contents of the above-mentioned communications are disclosed to the public by any means of communication.

Wiretapping can be performed either by technical devices or through the use of software (spyware). The blocking or interruption of communications ("Denial of service") may also consist of slowing down communications and can be achieved not only by using computer viruses, but also for example by causing system overload by generating a vast number of fake communications.

The offence is prosecutable on the action of the injured party; however, it is prosecutable ex officio where specific aggravating circumstances set out in the Article are met, including where the offence is committed against a computer or telecommunication system used by the State or by another public Entity or used by a company that provides public services or services of public interest, or where the offence is committed by abusing the role of system operator.

Within the company, the blocking or interruption of communications may for example be caused by the unauthorised installation of a software system by an employee.

Article 617-*quinquies* therefore punishes any person who, apart from cases permitted by law, in order to intercept communications relating to an IT or telematic system, or communications between several systems, or to prevent or interrupt said, obtains, possesses, reproduces, disseminates, imports, communicates, delivers, makes available in another way to others or installs equipment,

programmes, codes, key words or other means to intercept, prevent or interrupt said communications, regardless of the occurrence of such events. This offence is prosecutable ex officio.

Damaging computer information, data and programs (Article 635-*bis* of the Criminal Code)
Damaging computer information, data and programs used by the Government or any other public Entity or by an Entity providing public services (Article 635-*ter* of the Criminal Code)
Article 635-*bis* of the Criminal Code punishes, unless the deed constitutes a more serious offence, any person who destroys, damages, cancels, alters or suppresses computer information, data or software belonging to others.
According to a strict interpretation, the concept of "software belonging to others" might also include software used by the person under a licence granted by the lawful owners of the software.

Article 635-*ter* of the Criminal Code, unless the fact constitutes a more serious offence, punishes any conduct aimed at producing the occurrences described in the preceding Article, regardless of whether material damage actually occurs: any such material damage constitutes an aggravating circumstance. This offence applies only to conduct aimed at damaging computer information, data or software used by the Government or another public Entity or by an organisation providing a public service. Therefore this type of offence also includes conduct aimed at damaging data, information and software used by private organisations, where they are intended to provide public interest services.

Aggravating circumstances for both offences exist where the deed is committed with violence to individuals or threat, or by abusing the role of system operator. The first offence is prosecutable on the action of the injured party, or ex officio where one of the aggravating circumstances occurs; the second offence is always prosecutable ex officio.
If the conducts described are committed through unauthorised system access, they shall be punished under the above-mentioned Article 615-*ter* of the Criminal Code.

Damaging computer or telecommunication systems (Article 635-*quater* of the Criminal Code)
Damaging computer or telecommunication systems of public interest (Article 635-*quinquies* of the Criminal Code)
Article 635-*quater* of the Criminal Code, unless the fact constitutes a more serious offence, punishes any person who, by the conducts referred to in Article 635-*bis*, i.e. by introducing or transmitting data, information or software, destroys, damages or makes it impossible, either in whole or in part, to use another person's computer or telecommunication system or seriously obstructs its functioning.
For this offence to be committed, the system so attacked must be damaged or rendered unusable at least in part, or its functioning must be obstructed.

Article 635-*quinquies* of the Criminal Code punishes the same conduct set out in Article 635-*quater* even where no actual damage occurs. Where damage does in fact occur, this constitutes an aggravating circumstance (it should however be noted that the material obstruction to the system's functioning is not expressly included among the aggravating circumstances). For this Article to apply, the computer or telecommunications systems so attacked must be of public interest.
This provision, differently from Article 635-*ter*, contains no reference to use by Public Bodies: it would seem therefore that for this offence to occur, the systems attacked must simply be "of public interest"; therefore, on the one hand, their use by Public Bodies would not suffice, and on the other, the rule would also be applicable to systems used by private organisations acting for public interest purposes.

Both offences are prosecutable ex officio; aggravating circumstances occur where the deed is committed with violence to individuals or threat, or by abusing the role of system operator.

It would seem that the offence of system damage subsumes data and software damage where the latter have the effect of making the systems unusable or of severely obstructing their regular functioning.
If the conducts described are committed through unauthorised system access, they shall be punished under the above-mentioned Article 615-*ter* of the Criminal Code.

Unauthorized possession, distribution and installation of equipment, codes and other devices accessing computer or telecommunication systems (Article 615-*quater* of the Criminal Code)
Unauthorized possession, distribution and installation of computer equipment, devices or computer programs for the purpose of damaging or interrupting a computer or a telecommunication system's operations (Article 615-*quinquies* of the Criminal Code)
Article 615-*quater* punishes any person who, in order to obtain personal profit or profit for others or to cause damage to others, illegally possesses, produces, reproduces, distributes, imports, communicates, delivers, makes available to others or installs apparatus, instruments, parts of apparatus or instruments, codes, keywords or other methods suitable to access a computer or telematic system protected by security measures, or provides information for such purposes.
Article 615-*quinquies* punishes any person who illegally procures, possesses, produces, reproduces, imports, distributes, communicates, delivers or makes available in another way to others or installs computer equipment, devices or software in order to illegally damage a system or the data and software contained therein or to assist the interruption or the altering of such system's operation.
These offences, which are punishable ex officio, also occur in the event of unauthorised possession or dissemination of passwords or of potentially damaging programmes (virus, spyware) or devices

regardless of whether the other computer crimes illustrated above – which might be prepared by these actions – are actually committed or not.

One condition for the first offence is the intention of obtaining profit or causing damage. However, for the purpose of assessing such types of conduct, one key element might be the objectively abusive nature of the transmission of data, software, e-mail, etc., by persons who, while not intending to obtain profit or causing damage, are aware of the presence in such data etc. of a virus which might cause the harmful occurrences described in the provision.

Forgery of electronic documents (Article 491-*bis* of the Criminal Code)

Article 491-*bis* of the Criminal Code applies to public or private computer documents having probative value the same treatment applicable to forgery of traditional paper documents, as set out in Articles from 476 to 493 of the Criminal Code. They include in particular material falsification or provision of intentionally false statements committed by a Public Official or by a private individual, falsification of registers and notifications, intentionally false statements in certificates by providers of public interest services, and the use of a false act.

In current legislation, the concept of electronic document is independent of the material medium containing it, since the element having relevance in criminal law for the purpose of identifying the electronic document is whether such document can have probative value according to the rules of civil law[66].

In the offences of false deeds/forged deeds, one fundamental distinction must be made between material falsity and an intentionally false statement (falso ideologico): material falsity means the real author of the document is not the stated author, or that the document was altered (also by its original author) after being produced; an intentionally false statement occurs when the document contains untrue or unfaithfully reported statements.

As concerns computer documents having probative value, material falsity may occur where some other person's electronic signature is used, whereas alteration of the document subsequent to its preparation seems unlikely.

On the other hand, the provisions that punish the signing of blank sheets of paper (Articles 486, 487, 488 of the Criminal Code) do not seem to be applicable to electronic documents.

The offence of use of false acts (Article 489 of the Criminal Code) punishes any person who, while not taking part in the falsification of an act, uses such false act despite being aware of its falsity.

[66] On this point it should be noted that under the Digital Administration Code (Article 1, point p) of Legislative Decree 82/2005), an electronic document is "the electronic representation of acts, facts or data having legal significance", but:

- if such document is not signed with an electronic signature (Article 1, point q), it cannot have probative value, but can at the most, at the Court's discretion, satisfy the legal requirement of the written form (Article 20, paragraph 1-*bis*);
- where the document is signed with "simple" (i.e. unqualified) electronic signature it cannot have probative value (and for the purpose of assigning probative value the Court shall assess the objective characteristics of quality, security, integrity and inalterability of the electronic document);
- an electronic document signed with digital signature or any other kind of qualified electronic signature shall have the probative weight of a private deed as laid down in Article 2702 of the Civil Code unless a claim of falsity is made, if the signature is recognised by the person against whom the document is asserted.

Computer crime by the certifier of a digital signature (Article 640-*quinquies* of the Criminal Code)

This offence is committed by any person responsible for certifying electronic signatures and who, in order to gain an unjust profit for himself or for others or to cause damage to others, infringes the legal obligations concerning issuance of a qualified certificate[67]. The author of the offence can only be a "certification service provider" who performs specific certification functions in respect of qualified electronic signatures.

On this specific issue it should be noted that the Bank assumes the role of "certification service provider" and therefore is directly relevant to it. It should however be noted that in order to take on criminal relevance, the infringement of obligations relating to the issue of a qualified certificate must be accompanied by the specific intention described above (gaining an unjust profit or cause damage to others).

Obstructing procedures to define, manage and control the "National cyber security perimeter" (Article 1, paragraph 11, Law Decree 105/2019)

The crime punishes anyone who, in order to obstruct or influence the Authorities in charge of protecting the strategic technological infrastructure system:

1) provides information, data or factual elements not corresponding to the truth, which are significant:
   a) for preparing and updating lists of networks, systems (including the relative architecture and components) and IT services of the PA and of public and private operators based in Italy, on whom the operation of an essential State function or provision of an essential service for fundamental civil, social or economic activities depends, and of which the malfunction, interruption or misuse may harm national security;
   b) for the communications that the aforesaid public and private operations must provide to the CVCN (National Evaluation and Certification Centre, set up by the Ministry for Economic Development) of the supply contracts they intend stipulating to procure ICT assets, systems and services intended to be used with the aforesaid networks, systems and services;
   c) for carrying out audit and supervisory activities concerning compliance with provisions and procedures for the preparation and updating of the above lists, the notification of supplies and incidents and the security measures relative to the aforesaid systems, networks and services;
2) omits notifying the aforesaid data, information or factual elements within the times indicated.

* * *

Section II – Offences concerning non-cash payment instruments

[67] Under Article 1 points e) and f) of Legislative Decree 82/2005, qualified certificate means an electronic attestation which links a signature verification device to a person, confirms the identity of that person and meets the requirements laid down in Annex I to Directive 1999/93/EC and is provided by a certification service provider – i.e. a person providing electronic signature certification services or similar electronic signature related services – who fulfils the requirements laid down in Annex II to the same Directive.

Legislative Decree 184/2021 introduced, under predicate offences, the liability of the organization[68] for offences concerning non-cash payment instruments, and includes: the aggravating circumstance indicated in Article 640 *ter*, paragraph 2 of the Criminal Code, amendments to Article 493 *ter* of the Criminal Code, ex novo, Article 493 quater of the Criminal Code The characteristics and context of said offences are such they may be referred to the sensitive area of computer rimes, save - also in this case - for sensitive activities contemplated in this area, that includes offences which may generate unlawful income, are considered as intended to prevent money laundering offences in the broad sense.

The offences introduced by Article 25 *octies1* are indicated below:

Computer fraud that results in the transfer of cash, monetary value or virtual currency (Article 640 *ter*, paragraph 2).

Computer fraud, as already indicated in the section on offences against the Public Administration, consists of altering the functioning of an IT or telecommunications system or of tampering with the data, information or software contained therein, obtaining unfair profit. The aggravating circumstance that the fact produces a transfer of cash, monetary value or virtual currency also results in the liability of the Organisation, without the affected party being the State, Public Administration or the EU.

Unlawful use and counterfeiting of non-cash payment instruments (493 *ter* of the Criminal Code)

Any person who, in order to gain a profit, for themselves or others, unlawfully uses, not being the owner, credit or payment cards, or any other similar document that allows for the withdrawal of cash or purchase of goods or provision of services, or in any case any other non-cash payment instruments will be punished.

Any person who, in order to gain a profit, for themselves or others, counterfeits or alters the instruments or documents indicated above, or owns, sells or acquires instruments or documents of unlawful origin or that have been in any case counterfeited or altered, as well as the payment orders produced with said, will be punished.

The risk of committing this offence may in theory be present in all company contexts and in particular in all company processes concerned with the handling of cash flows, in relation to different types of non-cash payment instruments.

[68] See Article 25 octies.1 of Legislative Decree 231/2001.

In particular, all activities that make it possible to access identifying data, credentials, etc. functional to any improper use of payment instruments (other than case) owned by third parties, such as credit cards, are classified as sensitive activities.

Possession and distribution of IT equipment, devices or programs intended to commit offences concerning non-cash payment instruments (Article 493 *quater* of the Criminal Code)
Unless the fact constitutes a more serious offence, anyone who, in order to use or allow others to use, in committing offences concerning non-cash payment instruments, produces, imports, exports, sells, transports, distributes, makes available or in any way obtains for themselves or for others IT equipment, devices or programs which, due to the technical/construction or design characteristics, are mainly built to commit such crimes, or are specifically adapted for said purpose, will be punished.The conduct described could occur in the context of activities which involve the management and/or distribution of non-cash payment instruments and in technological environments supporting said activities.

Article 25 *octies*.1 of Legislative Decree 231/2001, has also extended the catalogue of predicate offences to “any other offence against the public faith, against assets or in any case that harms assets as set out in the Criminal Code”, on condition that “non-cash payment instruments” are concerned.

* * *

In general it should be noted that some types of computer crimes in concrete terms might well not fulfil the requirement of being committed in the Bank’s interest or for its benefit, which must be present for the Bank to incur administrative liability. However, where all the elements provided for by Legislative Decree 231/2001 occur, the Bank may be held liable, in accordance with the provisions of Article 8 of the Decree, even where the author of the offence cannot be identified (in this case, the offender, albeit unidentified, should at least be proven to be a manager or an employee). This eventuality is certainly not unlikely in the field of computer crime, in the light of the complexity of the medium and of the evanescence of cyberspace, which also make it objectively difficult to identify the specific place where the offence may have been committed.
Lastly, it should be recalled that Article 640-*ter* of the Criminal Code, which punishes computer crimes against the State or another Public Body, is already a predicate offence of the administrative liability of Organisations pursuant to Article 24 of Legislative Decree 231/2001 if committed against the State or another Public Body; on this point, the reader is referred to paragraph 7.2.1.

7.10.2 Sensitive company activities

The Bank's activities exposed to the risk of computer crimes (including the offences of "*Computer fraud that results in the transfer of cash, monetary value or virtual currency" and "Possession and distribution of IT equipment, devices or programmes intended to commit offences concerning non-cash payment instruments*" and the unlawful handling of electronic data held by the company refer to all company sectors where information technologies are used.

The Bank has put in place specific organisational safeguards and has adopted appropriate security solutions, in compliance with Supervisory Authority regulations and with the European and national regulations on data protection, to ensure prevention and control of risks relating to information technology (IT) and cyber security, to protect its information assets and customers and third parties.

The offence referred to in Article 640-*quinquies* of the Criminal Code concerns specifically the Bank's activity in its role as qualified certifier of digital signatures.

The sensitive activity identified by the Model where the risk of the above-described unlawful conduct is highest is the following:

- Management and use of the Group's IT systems and Information assets.

Lastly, as regards the offence of the *Unlawful use and counterfeiting of non-cash payment instruments*, and any other offence against the public faith, against assets or in any case that harms assets as set out in the Criminal Code, on condition that non-cash payment instruments are concerned, the Bank's sensitive activities during which this type of offence may be committed, concern all company processes that involve the handling of cash flows of the Bank and on behalf of its customers through different types of non-cash payment instruments, and related applications.

The sensitive activity identified by the Model where the risk of the above-described unlawful conduct is highest is the following:

- Management and use of non-cash payment instruments.

The protocols regulating other sensitive activities, such as the Management of procedures to purchase goods and services and professional services (section 7.2.2.8) and Combating terrorist financing and the laundering of proceeds from crime (section 7.6.2.1.) provide for some principles of control (for example monitoring operations intended to identify potential suspicious activity of customers), and of conduct, with preventive effects also in relation to said crimes.

We reproduce below the protocol laying down the control principles and rules of conduct applicable to this activity, as well as the detailed corporate regulations governing this activity.

Such protocols also apply to the monitoring of any activities performed by Group companies and/or outsourcers on the basis of special service agreements.

7.10.2.1. Management and use of the Group's IT systems and Information assets

Introduction

This protocol applies to all the Bank Structures involved in the management and use of the Group's computer systems and Information assets.

In particular, it applies to:

- all the Bank's structures involved in the management and the use of the information systems that interconnect with/use software of the Public Administration or the Supervisory Authorities;
- all the Structures tasked with designing, implementing or managing computer, technology or telecommunications tools;
- all the Structures responsible for implementing organisational, regulatory and technology actions to ensure the protection of the Group's Information assets in the activities falling under their competence and in relations with third parties with access to the Group's Information Assets;
- all the professional roles involved in company processes and operating therein for any reason, whether as employees or as collaborators or freelance professionals, who use the Bank's information systems and handle data belonging to the Group's Information Assets.

Pursuant to Legislative Decree 231/2001, the related processes might present opportunities for commission of the computer crimes referred to in Article 24-*bis*, and of the offence of "*Computer fraud",* laid down in Article 640-*ter* of the Criminal Code and referred to in Articles 24 and 25 octies.1 of the Decree (see sections 7.2.1 and 7.10.1) and of "*Possession and distribution of IT equipment, devices or programmes intended to commit offences concerning non-cash payment instruments*". Furthermore, access to the computer networks could also provide a means for committing offences against intellectual property rights[69].

The definitions given in this protocol are aimed at ensuring the Bank's compliance with applicable regulations and principles of transparency, correctness, objectivity and traceability in carrying out the activities concerned.

Process description

The use and management of computer systems and of Information Assets are essential activities for the performance of corporate business and characterise most of the Bank's processes.

The information systems used by the Bank also include hardware and software for fulfilment of requirements towards the Public Administration which involve the use of specific software supplied by the Public Bodies, or direct connection with such software.

[69] For a description of the relevant conduct see paragraph 7.10.

Hence the necessity to identify effective and stringent rules and measures relating to organisational, behavioural and technological security, and design specific control measures ensuring that the IT systems and the Group's Information Assets are operated and managed in full compliance with current legislation.

In the light of the above comments, the following processes have been identified for exercising control over the operation and management of the Group's IT systems and Information assets.

The computer security management process comprises the following phases:

- analysis of computer risk and identification of computer security requirements;
- management of Computer Resource Accesses and ICT Security Services;
- management of regulations and computer security architecture;
- monitoring IT security events and managing critical IT security events;
- third-party security (classification and monitoring of Parent Company suppliers);
- fostering of an IT security culture;
- design and implementation of computer security solutions.

The fraud prevention process involves the following phases:

- identification of the appropriate measures to upgrade prevention;
- monitoring of developments in computer crimes, also with regard to related physical security aspects;
- management of the activities necessary to identify and resolve threats to company assets;
- management of communications with Law Enforcement Bodies.

The physical security management process comprises the following phases:

- managing the protection of areas and premises where the activity is performed;
- managing the physical security of peripheral systems (premises of branches, central headquarters, other networks).

The process relating to the electronic signature certification service comprises the following phases:

- opening the contract;
- registering the holder;
- managing the certificate (suspending, reactivating, revoking, renewal and PIN unlocking).

The process for the design, development and implementation of the ICT services comprises the following phases:

- design, implementation and management of the Group's software solutions and technology infrastructure.

The ICT management and support process comprises the following phases:

- provision of ICT services;
- monitoring of the operation of ICT services and management of any malfunctions;
- user assistance via Help desk and problem solving activities.

The process to manage communications to the Authorities in charge of defining, managing and controlling the "National cyber security perimeter" comprises the following phases, in compliance with expected Government implementing measures:

- the identification of information and events that must be notified/reported;
- the transmission, depending on the relevant Authorities, of the communication/reporting, by competent functions.

The operating procedures for management of the processes described herein are governed by internal rules, which are developed and updated by the competent Structures, and which form an integral and substantive part of this protocol.

Control principles

Without prejudice to the specific security requirements applicable to the software of the Public Administration or the Supervisory Authorities used by the Bank, the control system safeguarding the processes described above must be based on the following factors:

- Authorisation levels defined within each operating step of the process described above. Specifically:
  - authorisations are managed by defining “access profiles” on the basis of the functions performed by each individual within the Bank;
  - changes to profile contents are performed by the Bank structures responsible for control of logical security, acting on the request of the Structure involved. The requesting Structure must in any case ensure that computer authorisations required match the work duties of each individual;
  - each user is associated with only one authorisation profile, on the basis of his role in the organisation and in compliance with the “least privilege” rule. In the event of user transfer or change of activity, a new authorisation profile will be defined, tailored to the newly assigned role;
  - entities enabled to manage communications to Authorities in charge of defining, managing and controlling the "National cyber security perimeter" are identified and authorised on the basis of the specific role assigned by the organisational code or by the Head of the reference Structure by means of an internal delegation, kept on file by the same Structure.

- Segregation of duties:
  - different roles and responsibilities are assigned in respect of information security management; in particular:

- Assigning specific responsibilities ensures control over the areas of security direction and governance and planning, implementation, operation and control of the countermeasures adopted to protect corporate Information Assets;
- precise responsibilities for the management of security issues are assigned to the organisational functions responsible for developing and managing information systems;
- responsibilities and mechanisms are defined to ensure the management of abnormal security events, emergency and crisis situations and communications to the relevant Authorities;
- precise responsibilities for preparing, validating, issuing and updating the security rules are assigned to corporate functions different from those in charge of computer security management;

- the activities of implementing and modifying software, managing computer procedures, physical and logical access controls and software security controls are organisationally assigned to structures which are different from the users, to ensure sound management and ongoing control over the information system management and use process;
- precise responsibilities are assigned to ensure that the software development and maintenance process, whether performed in-house or by third parties, is managed in a controlled and verifiable manner, following an appropriate authorisation process.

- Control activities: the management and use of the Bank's information systems and of the Group's Information assets undergo ongoing control activity by using appropriate information protection measures, so as to safeguard its confidentiality, integrity and availability, with particular reference to the handling of personal data, and by adopting for the overall set of corporate processes specific operating continuity solutions of a technological, organisational and infrastructural nature, able to ensure continuity in the event of emergency situations. These control activities also provide valid support ensuring traceability of all changes made to computer procedures, the identification of the users who have made such changes and of those who have carried out controls on the changes made.

  The planned controls, set out in the relevant internal policies, shall be based on identification of specific activities targeting long-term management also of the aspects relating to protection of the Group's Information assets, such as:
  - defining security objectives and strategies;
  - defining a risk analysis method for the Information Assets, to be applied to the company's processes and assets, estimating the greatest risks the information is exposed to with regard to the criteria of confidentiality, integrity and availability;
  - identifying appropriate countermeasures against the risk levels detected, monitoring and checking that such security levels are properly maintained;
  - delivery of appropriate staff training on computer security aspects in order to raise their awareness of and alertness to the issue;
  - preparing and updating security rules, in order to ensure their sustained applicability, adequacy and effectiveness;

- controls on correct application and compliance with the defined legislation.

The main control activities performed from time to time, and set out in detail in the reference internal rules, are the following.

With reference to physical security:

- protection and control of physical areas (perimeters/reserved areas) to prevent unauthorised accesses to, or altering or theft of information assets.

With reference to logical security:

- identification and authentication of user identification codes;
- authorising requests for access to information;
- provision of encryption and digital signature technologies to ensure the confidentiality, integrity and of stored of transmitted information and prevent its rejection.

With reference to the operation and management of applications, systems and networks:

- ensuring separation of the premises (development, testing and production) in which the systems and their applications are installed, managed and maintained, in order to ensure their sustained integrity and availability;
- preparing and protecting system documentation concerning configurations, customisation and operating procedures, to ensure the appropriate and secure performance of activities;
- putting in place of measures for software under development in terms of installation, management of operation and emergencies, and code protection, ensuring the preservation of the confidentiality, integrity and availability of the information handled;
- implementing actions to remove systems, applications and networks identified as obsolete;
- planning and managing the rescue of operating systems, software, data and system configurations;
- managing data storage devices and media to ensure their long-term integrity and availability by regulating and controlling use of the devices, equipment and all information assets assigned, and by defining procedures for the custody, re-use, reproduction, destruction and physical transport of removable data storage media in order to protect them from damage, theft or unauthorised access;
- monitoring applications and systems, by defining efficient criteria for the collection and analysis of the relevant data, in order to allow identification and prevention of non-compliant actions;
- prevention of malware by means of appropriate tools and infrastructure (including antivirus systems) and by assigning responsibilities and setting up procedures for the phases of installation, verification of new releases, updates and actions to be implemented when potentially damaging software is identified;
- formalising responsibilities, processes, tools and procedures for exchanging information by e-mail and through websites;
- adopting appropriate safeguards to achieve the security of telecommunications networks and supporting devices, and ensure the correct and safe circulation of information;

- establishing specific procedures covering the stages of system and network design, development and replacement, defining solution acceptance criteria;
- establishing specific procedures to ensure that any materials covered by intellectual property rights are handled in accordance with legal and contractual provisions;
- preparation and updating of specific technological and application inventories for the purposes of communication with the relevant Authorities.

With reference to application development and maintenance:

- identifying appropriate countermeasures and controls to protect the information handled by the applications, meeting the requirements of confidentiality, integrity and availability of the information handled, having regard to the areas and use procedures, integration with existing systems and compliance with the provisions of law and with internal rules;
- putting in place appropriate security controls throughout the application development process, to ensure their correct operation, including systems for restricting access to authorised persons only by means of tools, external to the application, for identification, authentication and authorisation.

With reference to the management of security failures:

- establishing appropriate reporting channels and procedures for promptly reporting incidents and suspicious situations, in order to minimise any consequent damage, prevent repetition of inappropriate conduct and initiate a response process which may also lead to declaration of a state of crisis.

With reference to the management of communications with the relevant Authorities:

- controls on the accuracy of communications with particular reference to the deadlines indicated for sending information, notifications and reporting incidents.

- Process traceability including both the electronic and the paper trail:
  - the decision-making process, with reference to the management and use of IT systems, is ensured by full system-wide traceability;
  - all occurrences and the activities carried out (including access to information, mitigation actions performed via the system, for example accounting adjustments, changes in user profiles etc.), with particular regard to the actions carried out by privileged users, are tracked through systematic recording (log file system);
  - all accesses to and exits from reserved areas by duly authorised staff who actually need to access such areas, shall be recorded by dedicated tracking mechanisms;
  - all operations performed on the data shall be tracked, compatibly with current laws, in order to allow reconstruction of the responsibilities and of reasons for the choices made; moreover each Structure shall be responsible for filing and storing the documentation it has produced, also in telematic or electronic format, which falls under its competence.

Rules of Conduct

The Bank's structures, howsoever involved in the activity of management and use of computer systems and of the Group's Information assets shall comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and any provisions of the Group's Code of Ethics and Internal Code of Conduct.

Specifically:

- the Structures involved in the processes shall prepare and maintain a census of the applications that interconnect with the Public Administration or with the Supervisory Authorities and/or of their specific software in use;
- all persons involved in the process must be duly appointed;
- each employee/system administrator shall report to Top Management any security incidents (including any attacks on the computer system by external hackers), making available and storing all documentation pertaining to the incident and setting in motion the response and escalation process, which may lead to declaring a state of crisis and notifications sent to the Relevant Authorities;
- each employee is responsible for the correct use of the computer resources assigned to him (e.g. desktop or laptop personal computers), which are to be used solely for performance of his work duties. Such resources shall be kept with due care, and the Bank must be informed without delay of any instances of theft or damage;
- where third parties/outsourcers are to be involved in the management of the Group's IT systems and Information assets and in the interconnection with/use of the software of the Public Administration or the Supervisory Authorities, the contracts entered into with such persons shall contain a specific declaration that they know the provisions of Legislative Decree 231/2001 and undertake to comply with them;
- the payment of fees or compensation to external collaborators or consultants involved is subject to permission given in advance by the organisational unit responsible for assessing service quality and the resulting fairness of the fee demanded; in any case, no remuneration shall be payable to employees or external consultants where not fully justifiable by the type of work performed or to be performed.

With reference to the specific activity of "qualified certifier"

- at the time of signing the contract and handing over the electronic signature device each employee shall verify the customer's identity by demanding presentation of a legally recognised and valid identity document and, if the person acts on behalf of third parties, by verifying that he holds the required power of attorney;
- the operator must ensure the sound and prompt performance of the operations relating to the certificate (suspension, reactivation, revocation, renewal and PIN unlocking).

In any case, it is forbidden to engage/collaborate in or induce conduct which may belong to one of the types of offences covered by Legislative Decree 231/2001; more specifically, purely by way of example and without limitation it is forbidden to:

- enter without authorisation, directly or through another person, into a computer or telematic system protected by security measures against the will of the holder of access rights, also in order to acquire confidential information or to unduly use, counterfeit or alter non-cash payment instruments;
- access the Bank's or the Group's computer system or telecommunications system or part thereof, or databases or parts thereof, without holding credentials or using the credentials of authorised colleagues;
- fraudulently wiretap and/or disclose to the public through any information system, communications within a computer system or telecommunication system or between several systems;
- use unauthorised technical devices or software tools (viruses, worms, trojans, spyware, diallers, keyloggers, rootkits, etc…) able to hinder or interrupt communications within a computer or telecommunications system or between several systems;
- destroy, damage, cancel, alter or suppress information, data or software programs owned by third parties or endanger the integrity and the availability of computer information, data or software used by the Government or another public Entity or relating to them or howsoever of public interest;
- introduce or transmit data, information or programmes to destroy, damage, make entirely or partially unusable, or prevent the functioning of information or computer systems of public utility;
- hold, procure, reproduce or disseminate access codes or other suitable means of access to a system protected by security measures without authorisation;
- produce, import, export, sell, transport, distribute, make available or in any way obtain for themselves or for others IT equipment, devices or programs which are mainly designed to commit crimes concerning non-cash payment instruments or are adapted for said purpose;
- procure, reproduce, disseminate, communicate, or make available to others computer equipment, devices or software in order to illegally damage a system or the data and software contained therein or to assist the interruption or the altering of such system's operation;
- alter electronic documents by using another person's electronic signature or by any other means;
- produce and transmit electronic documents containing false and/or altered data;
- carry out, through access to a computer network, unlawful conduct constituting breaches of intellectual property rights, including, for instance:
  - dissemination in any form of intellectual property not intended for publication or misappropriate their authorship;
  - copying, holding or disseminating in any form without being authorised computer programmes or audiovisual or literary works;
  - retaining any means intended to remove or circumvent the protective devices of processing programmes;
  - reproducing databases on media not marked by the Italian Society of Authors and Publishers (SIAE), disseminating them in any form without the copyright holder's authorisation or in breach of the prohibition established by the maker;

  - removing or altering digital information entered in protected works or appearing in disclosures to the public, concerning relative rights;
  - importing, distributing, installing, selling, modifying or using devices for unscrambling restricted access audiovisual transmissions, also where these are receivable free of charge.
- failing to notify within the deadlines indicated by applicable regulations on "national cyber security", significant data, information or factual elements;
- presenting documents and data that are incomplete and/or communicating false or altered data in communications concerning "national cyber security".

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.10.2.2. Management and use of non-cash payment instruments

Introduction

This protocol applies to all the Bank structures involved in the management and use of non-cash payment instruments.

The Bank is continually committed to searching for and adopting operating solutions which are as updated as possible, aiming to prevent and obstruct the fraudulent use of payment instruments and therefore the execution of unauthorised payment transactions.

Pursuant to Legislative Decree 231/2001, the process could represent opportunities to commit the offence of the "*Unlawful use and counterfeiting of non-cash payment instruments*", and any other offence against the public faith, against assets or in any case that harms assets as set out in the Criminal Code, on condition that non-cash payment instruments are concerned.

The definitions given in this protocol are aimed at ensuring the Bank's compliance with applicable regulations and principles of transparency, correctness, objectivity and traceability in carrying out the activities concerned.

Process description

The process to manage and use non-cash payment instruments comprises the following process:

- Payment cards (debit and service cards, credit cards, prepaid cards);
- Inflows and payments (e.g. cheques, bank transfers, direct debits, cash orders, payments by notification – bills);
- Services to Access Digital Channels (access and remote identification of natural and legal persons, other services);
- Fraud prevention (Security Fraud Management);
- Management of Claims, Complaints and Derecognition (Customer Relationship Management);

Management of human resources with reference to company credit cards, meal vouchers, service cards for vehicles (fuel cards, motorway tool automatic payment systems), issued to Bank employees.The operating procedures for management of the processes described herein are governed by internal rules, which are developed and updated by the competent Structures, and which form an integral and substantive part of this protocol.

Control principles

The control system for monitoring the processes described above must be based on the following elements:

- Defined authorisation levels. Specifically:
  - persons exercising authorisation powers (including the management of unauthorised transactions, fraud and derecognitions) and/or negotiation powers in the management of pre-contractual relations concerning the protocol in question:
    - are identified and authorised on the basis of their specific role assigned by the organisational code or by Head of the reference Structure by means of internal delegation, to be kept on file by the same Structure;
    - only operate within the scope/portfolio of customers assigned to them by the Head of the reference Structure;
  - authentication mechanisms are identified based on the risk of transactions concerning non-cash payment instruments.
- Segregation of duties:
  - determined responsibilities are assigned in the management of the management process:
    - payment cards - including company credit cards - through the definition of duties and specific controls on the issue, delivery, replacement, renewal, activation, withdrawal, waiver or termination of the customer or employee;
    - cheques (issue, management of procedural blocks and/or limitations on the issue of cheques, management of reporting to the Interbank Database on Cheques and Credit Cards, management of obligations in the event of loss, theft or destruction);
    - digital channels (activation of the service, management of credentials including blocks);
    - fraud (monitoring of anomalous or suspicious transactions, precautionary or final block of payment instruments etc.);
    - derecognitions of payments that are undertaken by entities other than those appointed for the commercial development of products/services.

- Control activities:
  - adoption of organisational and technological measures:
    - for the analysis of events occurring and threats, to under the risks and types of fraud in order to increase capacity to identify and prevent criminal events;
    - for the management of requests from customers to recover authentication mechanisms relating to non-cash payment instruments;
    - for the management of inventories of prepaid cards, debt and service cards, and in particular, for the periodic balancing of card and any hard copy PINs;
    - for the payment of cheques drawn on the Bank (identification of the presenting party, the validity of the cheque and signatures, existence of any operating blocks);
    - control on compliance with external regulatory provisions during the planning of new products and/or services connected with non-cash payment instruments.

- Process traceability including both the electronic and the paper trail:
  - use of IT systems supporting operations, to ensure that the data and information relating to the procurement process are recorded and kept on file and the use of non-cash payment instruments and, in particular, of unauthorised transactions, fraud and derecognition activities;
  - in order to allow a clear understanding of the responsibilities and the motives behind the choices made, the Structures - from time to time involved in the management of non-cash payment instruments and, in particular, unauthorised transactions, fraud and derecognition activities - shall be responsible for archiving and retaining the documentation produced also by telematic or electronic means, in relation to carrying out duties as part of the management of the activities described above.

Rules of conduct

The Bank's Structures, howsoever involved in activities to manage and use non-cash payment instruments, shall comply with the procedures set out in this protocol, with the applicable provisions of law, internal rules and any provisions of the Group's Code of Ethics and Internal Code of Conduct. Specifically:

- persons exercising authorisation powers (including the management of unauthorised transactions, fraud and derecognitions) and/or negotiation powers in the management of pre-contractual relations shall be specifically appointed;
- if third parties/outsourcers are to be involved in the management of non-cash payment systems, the contracts entered into with such persons shall contain a specific declaration that they know the provisions of Legislative Decree 231/2001 and undertake to comply with them;
- all employees must immediately report to their superior any attempt at counterfeiting and any improper use of non-cash payment instruments by customers or third parties which they become aware of. The superior shall in turn forward the report received to the Internal Auditing Structure for appropriate assessment and the completion of any formalities to the Surveillance Body in accordance with the provisions under Chapter 4.1.

In any event, it is forbidden to initiate, cooperate/give rise to conduct that could be considered an offence in terms of Legislative Decree 231/2001, and, more specifically by mere way of example, to:

- unduly use and/or promote the improper use by third parties who are not owners of payment cards, or any other similar document that allows for the withdrawal of cash or purchase of goods or provision of services, or in any case any other non-cash payment instruments;
- counterfeit or alter non-cash payment instruments,

- possess, sell or acquire non-cash payment instruments or documents of unlawful origin or that have been in any case counterfeited or altered, as well as the payment orders produced with said;
- enter without authorisation, directly or through another person, into a computer or telematic system protected by security measures against the will of the holder of access rights, also in order to unduly use, counterfeit or alter non-cash payment instruments.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.11 Sensitive area concerning crimes against industry and trade and crimes involving breach of copyright and customs' law

7.11.1 Types of offences

Introduction

Law 99 of 23.7.2009 – Provisions for the development and internationalisation of enterprises, and measures on energy – under a broad framework of initiatives to re-vitalise the economy and protect the authenticity of the "Made in Italy" label, and safeguard the interests of consumers and competition, has included a number of offences within the sphere of the liability of Entities, including certain offences introduced or reformulated by the same law. In particular, in the amended version of Legislative Decree 231/2001, Articles 25-*bis* and 25-*bis*.1 refer to offences set out in the Criminal Code relating to industry and trade[70], while Article 25-*novies* in order to strengthen the fight against intellectual property piracy[71] and counter the serious economic damage it causes to authors and to the related industry – refers to offences set out in the copyright law (Law 633/1941).

Smuggling crimes are included in the aforementioned provisions, introduced in Article 25-sexiesdecies[72] in order to implement the provisions of European legislation aimed at protecting the interests of the public finance of the European Union.

The offences in question are described below.

Counterfeiting, alteration or use of distinctive marks of intellectual works or industrial products (Article 473 of the Criminal Code)

The offence is committed by any person who, despite being able to ascertain that trademarks and other distinctive marks of industrial products belong to other parties, counterfeits them, or alters the original marks, or uses counterfeit marks without having taken part in their counterfeiting[73].

[70] Subsequent to the amendment introduced by Law 99/2009, Article 25-*bis* of Legislative Decree 231/2001 – which formerly only concerned counterfeiting of money and official stamps – has been extended to cover the crimes set out in Articles 473 and 474 of the Criminal Code, which share with the former the legal asset which is mainly protected, i.e. the public trust, seen as the confidence that the public places in the genuineness of specific objects, marks or logos.

[71] Pursuant to Article 1 of Law 633/1941, intellectual works protected by copyright are those belonging to literature (including scientific and educational literature), music, the figurative arts, architecture, theatre, and film, irrespective of their form of expression. Computer software and data banks which by their choice of arrangement of materials constitute an intellectual creation of their author are also ranked as literary works.

[72] See Article 5 of Legislative Decree 75/2020

[73] The term "use" of the counterfeit marks means ancillary types of conduct, such as, for instance, placing on one's products counterfeit marks which have been falsified by third parties. In other words, it concerns types of conduct different from either putting into circulation products bearing counterfeit marks, covered by Article 474 of the Criminal Code, or from those conducts specifically related to counterfeiting, such as reproducing another party's mark in one's advertising, in commercial correspondence, in websites etc.

Counterfeiting occurs where a mark is reproduced faithfully or its essential elements are imitated so as to appear authentic on initial perception. These are classified as material falsifications likely to harm public reliance on the fact that the products or services so marked come from the company which is the holder, licensee or concessionaire of the registered mark. According to case law marks still unregistered are also protected, where an application has already been filed, since such application makes it formally knowable. For this conduct to constitute an offence, it must be engaged in intentionally; intention may also exist where the author of the conduct, while not having the certainty that the mark has been registered (or that an application for registration has been filed), fails to implement the appropriate checks despite having reason to harbour such doubt.

The second paragraph punishes the conduct of counterfeiting, as well as the use, by another party who did not take part in the counterfeiting of patents, designs and industrial models belonging to others[74]. This Article too aims at combating material counterfeiting which, in this type of offence, concerns documents proving the granting of the patents or model registrations. On the other hand, violation of the rights of exclusive economic exploitation of a patent is punishable under Article 517-ter of the Criminal Code.

Introducing into the country and selling products bearing counterfeit marks (Article 474 of the Criminal Code)

Article 474 of the Criminal Code punishes the conduct of those who, not having committed the offences covered by Article 473 of the Criminal Code, introduce into the territory of Italy industrial products bearing counterfeit or altered marks or distinctive signs, or hold for sale, sell or howsoever put into circulation counterfeit products, if they are not already punishable for having introduced them into the territory of Italy. To give rise to this offence, the conduct must be aimed at gaining a profit.

The holder of such products may be punishable, in addition to the offence in question, also for receipt of stolen goods, if at the time of purchasing the products he was aware of the falsity of the distinctive signs placed on the product by his supplier or by another party. It should be noted that, pursuant to Article 25-*octies* of the Decree, the offence of receipt of stolen goods may also give rise to the administrative liability of Entities.

Infringement of the freedom of commerce or industry (Article 513 of the Criminal Code)

This offence, prosecutable on the injured party's action, is committed by the exercise of violence against property or the use of fraudulent means to prevent or disrupt the operation of an industry or commerce, unless a more serious offence is committed (e.g. arson, or one of the computer crimes set out in Article 24-*bis* of the Decree). For instance, this offence has been deemed to occur by those

[74] The Intellectual Property Code (Legislative Decree 30/2005), states in Article 2: "Patenting and registration give rise to intellectual property rights. The following can be covered by patents: inventions, utility models, new varieties of plants. The following can be registered: marks, designs and models, and topographies of semiconductor products".

who enter in their website's source code – for the purpose of enhancing its visibility for search engines – keywords referable to a competitor's enterprise or products, in order to divert such competitor's potential customers.

Illegal competition through threats or violence (Article 513-*bis* of the Criminal Code)

This offence occurs when a businessperson carries out acts of competition using violence or threats. This provision introduced into the Criminal Code by the anti-mafia law "Rognoni – La Torre" 646/1982, can also apply outside the scope of mafia-type criminal associations; its purpose is to combat acts aimed at preventing or limiting the market activities of competitors. The offence also occurs when the violence or threat is committed by third parties on behalf of the businessperson, or is not directly directed at the competitor but rather at his potential customers. Cases of such offences may include for instance: the threat of unfair damage to the participants in a public call for tenders in order to be informed of the contents of their tenders and submit a lower-priced tender; a threat to one's customer to apply worse terms and conditions or revoke granted credits or, in relations with one's supplier a threat to refrain from placing other orders in the event that the customer/supplier uses the services/supplies of a specific competitor.

Fraud against national Industries (Article 514 of the Criminal Code)

This offence occurs when harm is done to national industry by placing on sale or otherwise putting into circulation, industrial products with counterfeited trademarks or distinctive marks. The scope of the damage must be such as to harm not only individual enterprises, but the whole industrial economy of Italy.

Fraud in the conduct of commerce (Article 515 of the Criminal Code)

Unless the conduct gives rise to an offence of fraud, this offence is committed by a person engaged in commercial activity who delivers goods other than those agreed, or delivers goods which, while being of the same species as the agreed upon goods, differ from them as to origin, provenance, quality or quantity.

Sale of non-genuine foodstuffs as genuine (Article 516 of the Criminal Code)

The offence is committed by any person who sells or places on the market non-genuine foodstuffs, i.e. substances, foods and beverages intended for human consumption which, while not hazardous for health, have been altered by adding or removing elements, or have a different composition from that required.

Sale of industrial products with deceptive marks (Article 517 of the Criminal Code)

This offence is committed by placing for sale or otherwise putting into circulation intellectual works or industrial products bearing names, trademarks or distinctive marks[75] likely to mislead the buyer about the origin, provenance or quality of the work or product. The offence occurs where the distinctive marks, also having regard to the other circumstances of the concrete case (price of the products, their characteristics, manner of placing for sale) are likely lead the consumers to confuse the products with similar products (but of different origin, provenance or quality) bearing a genuine mark. The provision safeguards correct commercial practices and is applicable in the alternative, where the conditions for the more serious offences set out in Articles 473 and 474 of the Criminal Code are not met. It includes cases such as the counterfeiting and use of non-registered trademarks, the use of or packages with original trademarks but containing different products, and the use of the trademark by the lawful trademark holder on products whose quality standards differ from those of the products originally bearing the trademark (the conduct does not constitute an offence where production is contracted to another company but the client controls compliance with his quality specifications).

Manufacture and sale of goods made by usurping industrial property rights (Article 517-*ter* of the Criminal Code)

The offence covers two different types of conduct. The first, prosecutable on the injured party's action, occurs when any person, being able to learn of the existence patents or registrations held by other parties, manufactures or uses for industrial manufacturing purposes items or other goods, thereby usurping or violating an industrial property right. If the conduct includes the counterfeiting of trademarks or another of the conducts laid down in Articles 473 and 474 of the Criminal Code, the perpetrator might also be prosecutable for such offences.

The second type of offence occurs when a person, in order to make a profit, introduces in the territory of Italy, holds for sale, places for sale or otherwise puts into circulation goods manufactured in infringement of industrial property rights. If the goods bear counterfeit marks, Article 474, paragraph 2, of the Criminal Code shall also apply.

Counterfeiting of geographical indications or denominations of origin of agricultural food products (Article 517-*quater* of the Criminal Code)

This offence consists in counterfeiting and altering geographical indications or designations of origin of agricultural food products[76] and, for the purpose of making a profit, introducing in Italy, holding for

[75] Article 181-*bis*, paragraph 8, of Law 633/1941 states that for the purposes of criminal law the SIAE mark is considered a distinctive mark of an intellectual work.

[76] Pursuant to Article 29 of Legislative Decree 30/2005 the following are protected: "geographic indications and designations of origin which identify a country, region or locality, when they are adopted to designate a product that originates from such places and whose quality, reputation or characteristics are exclusively or essentially linked to the geographical environment of origin, inclusive of natural, human and traditional factors".

sale, offering for sale and offering directly to consumers or putting into circulation such products bearing counterfeit indications or designations.

Making available protected intellectual works in telecommunications networks without authorisation (Article 171, paragraph 1 point a-*bis*, Law 633/1941)

Aggravated unauthorised use of protected intellectual works (Article 171, paragraph 3, Law 633/1941)

The first offence occurs when any person, without being authorised, for any purpose and in any form, makes available to the public a protected intellectual work, or a part thereof, by placing it in a system of telecommunications networks through connections of any kind. In certain specific cases – for cultural purposes or purposes of free expression and information, and subject to certain limitations – it is permissible to disclose others' intellectual works to the public[77].

The second offence consists of the unauthorised use of others' intellectual works (by means of reproduction, transcription, dissemination in any form, placing for sale, placing on telecommunications networks, public performance or representation, creative uses such as translations, summaries, etc.); this offence is aggravated by the harm to the author's non-material rights. In this case, the conduct which already constitutes an offence is aggravated by the prohibition of publication imposed by the author, or by usurping authorship (plagiarism), or by deforming, altering or otherwise changing the work in a way that harms the author's honour or reputation.

Both of the above offences apply in the alternative when the conduct is not characterised by profit-making aims, in which case the conduct would be punished, more severely, under the types of offence set out in Articles 171-*bis* and 171-*ter*.

Abuses concerning software and databases (Article 171-*bis* of Law 633/1941)

The first paragraph of the Article, which refers to computer software[78], punishes the conducts of unauthorised duplication and import, distribution, sale, holding for commercial or business purposes (hence also for internal use within one's undertaking) and leasing, when such conducts concern software contained in media not bearing the SIAE mark (Italian Society of Authors and Publishers). This offence also occurs when a person prepares, holds or exchanges any means aimed at removing or circumventing software protection devices.

[77] See, for instance, Article 65 of Law 633/1941, which provides that current event features published in magazines and newspapers may be used by third parties, unless their reproduction has been expressly forbidden, provided their source, date and author are indicated.

[78] Pursuant to Article 2, no. 8 of Law 633/1941 computer software in any form is protected, as long as it is original, which are an intellectual work of their author. The term software includes the preparatory materials for designing such software. Articles 64-*bis*, 64-*ter* and 64-*quater* of the above-mentioned law regulate extension of the software author's rights and cases where the software may be freely used, i.e. the instances where reproductions or actions on the programme are permitted even without the right-holder's specific authorisation.

The second paragraph, which concerns protection of a database author's copyright[79], punishes the permanent or temporary, total or partial reproduction of such database, by any means and in any form – on media not bearing the SIAE mark, and its transfer onto another medium, its distribution, public communication, presentation of demonstration, if not authorised by the copyright holder. This offence also covers the conduct of duplicating and reusing all or a significant part of the database contents, thereby infringing the prohibition imposed by the establisher[80] of the database. "Duplicating" means a permanent or temporary transfer of data onto another medium, by any means and in any form; "reusing" means any form of making the data available to the public, including by distributing copies, rental, or transmission by any medium and in any form.

All the above-mentioned conducts must be characterised by the specific intention of making a profit, i.e. achieving an advantage, which may also consist of saving costs.

Abuses concerning audiovisual or literary works (Article 171-*ter* of Law 633/1941)

This provision lists a long series of unlawful conducts – where committed for non-personal use and for profit-making purposes – concerning: works intended for television, cinema, sale or hire; disks, tapes or similar media or any other media containing audio clips or video clips of musical, film or similar audiovisual works or sequences of moving images; literary, dramatic, scientific or educational works, musical or musical drama works or multimedia works. The punished conducts include:

- unauthorized duplication, reproduction, transmission or public dissemination using any procedure;
- the following conducts, engaged in by a person who did not take part in the unauthorised duplication or reproduction: introducing in Italy, holding for sale or distribution, placing on sale, supplying, screening in public or broadcasting on television or radio, or playing in public the unauthorised copies or reproductions;
- the same conduct listed in the above bullet point (except for introducing in Italy and playing/screening in public) is punished when it involves the use of any media – even when not obtained by unauthorised duplication or reproduction – not bearing the required SIAE mark or which bears a counterfeit mark.

The following abuses are also prosecutable: the dissemination of services provided with unscramblers of encrypted transmissions; the trafficking in devices which enable unauthorised access to such services or products aimed at circumventing the technology safeguards preventing

[79]Under Article 2, no. 9, of Law 633/1941, databases consist of collections of works, data or other independent elements, systematically or methodically arranged and which can be accessed by individuals using electronic or other means. This provision clearly leaves unprejudiced the separate protection granted to any copyright existing on intellectual works which may be present in the database. Articles 64-*quinquies* and 64-*sexies* of the law regulate the extension of the database author's copyright and the cases where the database can be freely used.

80 The right of the establisher of the database are regulated by Articles 102-bis and 102-ter of Law 633/1941. The word "establisher" designates the party who made substantial investments in order to create, verify or presenting a database and who, independently of the protection granted to the database author in respect of the creative criteria according to which the material was selected and arranged, has the right to forbid the duplication or reuse of all or a significant part of the database contents. With regard to databases available to the public, for example by means of free online access, the users, also without the establisher's express authorisations, may duplicate or reuse non-significant parts of such databases' contents, in qualitative and quantitative terms, for any purpose, except where such duplication or reuse have been expressly forbidden or limited by the establisher.

unauthorised uses of protected works; removing or altering electronic copyright notices present in the protected works or appearing in notices to the public; or importing or putting into circulation works from which the above-mentioned copyright information has been deleted or altered.

Failure to make communications or making false communications to SIAE (Article 171-*septies* of Law 633/1941)

This offence is committed by any manufacturers or importers of media containing software intended for sale who fail to provide SIAE with the data necessary to identify the media in respect of which they wish to avail themselves of exemption from the obligation to affix the SIAE mark[81].

The offence also includes providing a false declaration of compliance with legal obligations to SIAE in order to obtain the SIAE marks to be placed on the media containing software or audiovisual works.

Fraudulent unscrambling of restricted-access transmissions (Article 171-*octies* L. 633/1941)

This offence is committed by any persons who, for fraudulent purposes, produces, imports, distributes, installs, places on sale, modifies or uses, also for personal use only, devices for unscrambling restricted access audiovisual transmissions, also where these are receivable free of charge.

Smuggling crimes (Legislative Decree 43/1973).

These provisions punish a structured set of behaviour which, in brief, has the aim of avoiding paying border duties on goods.

Border duties mean import and export duties, levies and other taxes on exports or imports required under EU regulations, monopoly rights, border surcharges and any other consumption tax or surcharge in favour of the State.

7.11.2 Sensitive company activities

With reference to banking operations, crimes against industry and trade and crimes involving breach of copyright are more likely to occur in the following areas:

- in relationships with customers, having regard to the granting of financing or to provision of services to persons involved in the unlawful activities in question;

[81] Under Article 181-*bis*, paragraph 3 of Law 633/1941, without prejudice to compliance with the rights protected by the law, the SIAE mark need not be affixed to media containing software to be used solely via a computer and not containing any audiovisual works other than works created expressively for the computer software, and not containing reproductions exceeding 50% of pre-existing audiovisual works, giving rise to competition in their use for profit-making purposes.

- in the participation in public competitive tendering procedures, with particular regard to unlawful conduct towards participants;
- in the procurement or use of products, software, databases and other intellectual works to be used in Bank activities or intended as gifts for customers;
- in the granting to commercial partners of material or digital space for sales and promotional purposes.

A lower degree of risk is associated with the development and launch of new products, with management of the Group's naming and trademarks, external communication or advertising and marketing initiatives, or with customer relationship management based on the principles of fair competition and correct and transparent commercial practices, and this by reason of the well-developed system of safeguards and control procedures already laid down in the sectorial legislation.

Accordingly, reference is made to the applicable protocols:

- paragraph 7.6.2.1 on "Financial fight against terrorism and money laundering";
- paragraph 7.2.2.8 on "Management of the procedures for the procurement of goods and services and for the appointment of professional consultants";
- paragraph 7.2.2.9 on "Management of gifts, entertainment expenses, donations to charities and sponsorships";
- paragraph 7.10.2.1 on "Management and use of the Group's IT systems and Information assets";
- paragraph 7.2.2.1 on "Signing contracts with the Public Administration", the above protocols contain processes, control principles and rules of conduct which are also aimed at preventing commission of the offences covered by this paragraph.

With regard to smuggling crimes, the risks of committing said may arise in the context of banking activities relative to processes for the procurement of imported goods, as well as of a more general nature in obligations with the customs authorities. Accordingly, reference is made to the applicable protocols:

- paragraph 7.2.2.3. "Management of activities connected with the application for authorisation or the implementation of obligations vis-à-vis the Public Administration";
- paragraph 7.2.2.8 "Management of the procedures regulating the provision of goods and services and professional appointments";

which contain principles of control and conduct that are effective in preventive times, also in relation to the aforementioned crimes.

Such protocols also apply to the monitoring of any activities performed by Group companies or outsourcers on the basis of special service agreements.

7.12 Sensitive area concerning environmental crimes

7.12.1 Type of offence

Introduction

Article 25-*undecides* of Legislative Decree 231/2001 identifies offences against the environment, for which, based on Community law provisions, entities are administratively liable[82].

These offences are described in the Italian Criminal Code, in Legislative Decree 152/2006 (Environment Protection Policy, hereinafter referred to as EPP) and in various special laws, both classified as criminal offences as well as contraventions[83]. These cases are the following:

Environmental pollution (Article 452-*bis* of the Criminal Code)

The regulation punishes all those who unlawfully endanger or bring about a significant and measurable deterioration of water, of air, of the soil or subsoil, of an ecosystem or of the biodiversity.

Environmental disaster (Article 452-*quater* of the Criminal Code)

The regulation punishes all those who unlawfully provoke an environmental disaster, that consists in the irreversible alteration of the equilibrium of ecosystem, or the elimination of which is particularly burdensome and exceptional, or in harm to public safety based on the severity of the event, the extension or effects, or due to the number of persons harmed or exposed to hazard.

Traffic and abandonment of highly radioactive material (Article 452-*sexies* of the Criminal Code)

Diverse unlawful conduct (disposal, purchase, receipt, transport, import, export, detention, abandonment, etc.) involving highly radioactive materials is punished.

Criminal association with aggravating circumstances regarding the environment (Article 452-*octies* of the Criminal Code)

The regulation anticipates specific aggravating circumstance for the penalty for crimes of criminal association having the goal of committing any of the environmental offences provided for by the

[82] Article 25-*undecies* of Legislative Decree 231/01, in force since 16 August 2011, in the text first included by Legislative Decree 121/11 enacted for the application of Directive 2008/99/EC and 2009/123/EC on the protection of the environment through criminal law and Directive 2009/123/EC and subsequently amended by Law 68/15, in force since 29 May 2015, that introduced new environmental crimes in the Criminal Code.

[83] The offences are those listed in the Criminal Code (except for Articles 727-bis and 733-bis and by the EPP in articles 258 sub-article 4, 2nd part, 260 paragraphs 1 and 2, 260-bis sub-articles 6, 7 and 8 and document forgery to trade in animal and plant species and the offence of wilful pollution by ships. As a general rule, the essential elements of a crime are punished even if committed work orders by way of negligence; the crimes of pollution, contamination and environmental disaster, if committed through negligence, are punished pursuant to Article 452-quinquies of the Criminal Code and constitute and also constitute predicated crimes with administrative liability for Entities.

Criminal code. If involving a "*mafia-type association*", the fact itself of acquiring the management or control of an economic activity, of concession, of authorizations, authorisations, public tenders, or of public services regarding environmental matters is an aggravating circumstance.

Offences involving protected wild animals or plants or protected habitats (articles 727-*bis* and 733-*bis* of the Criminal Code)

The capture, possession, killing or destruction of specimens pertaining to species of protected wild animals or plants shall be punishable, excluding cases where this is allowed by law or where the damage is considered negligible in terms of the quantity of specimens involved or in terms of the impact on the preservation of the species. Also punishable is destruction or damage that endangers the conservation status of a habitat inside a protected site. Community rules list the protected animal and plant species and identify the characteristics which impose that local laws classify a natural habitat or the habitat of species as a special protection area or special area of conservation.

Breach of rules regulating discharges (article 137, sub-articles 2, 3, 5, 11 and 13, EPP)

Article 137 EPP punishes a series of violations of the rules on waste water, and in particular: unauthorised discharges of industrial waste water containing specific hazardous substances, or in contravention of the provisions contained in the authorisation or notwithstanding its suspension or revocation, and discharges of hazardous substances beyond the established limits; breach of discharges restrictions on the ground, in groundwater and underground, except in the cases contemplated under articles 103 and 104 EPP.

Lastly, breach of rules prohibiting discharges into sea of hazardous substances by ships or aircrafts, as defined in international treaties is also punishable, save for authorized discharges of rapidly biodegradable quantities.

Breach of waste management regulations (article 256, sub-articles 1, 3, 5 and 6, 1st part, EPP)

Punishable deeds are waste collection, transport, retrieval, disposal, sale or brokerage in the absence of the necessary licences, enrolment in the national Register of waste management bodies and notification to the competent authorities or in contravention of provisions included in the licences issued or communicated by the authorities or in the absence of the applicable requirements.

Moreover, unauthorised activities involving the creation or management of a waste tip, mixture of different types of hazardous waste either amongst themselves or with waste which is not hazardous and the deposit of hazardous medical waste at the place of production of a quantity exceeding 200 litres, or equivalent quantity, are also punishable.

Failure to conduct remediation for cases of ground, underground, surface water or groundwater pollution (article 257, sub-articles 1 and 2, EPP)

Unless the fact constitutes a more serious crime (e.g. referred to above in Article 452- *bis* of the Criminal Code), anyone who has caused the pollution in question by exceeding the risk threshold concentrations and does not arrange for the necessary communications to the competent authorities and the clean-up of the site pursuant to Article 242 of the EPP is liable to be punished. Clean-up actions are a condition of non-punishment also for the environmental fines envisaged by other special laws for the same event.

False certification of waste analysis (article 258, sub-article 4, 2nd part, EPP)[84]

Whosoever provides false information on the nature, composition and chemical-physical properties of waste shown on the waste analysis certificate and whosoever utilises a false certificate for the transport of waste shall commit this offence.

Illegal shipment of waste (article 259, sub-article 1, EPP)

The regulation punishes whosoever makes a cross-border shipment of waste in breach of EU Regulation No 259/93, which was repealed and substituted by EU Regulation No 1013/2006.

Activities organised for the illegal trafficking of waste (article 452- *quaterdecies*, sub-articles 1 and 2 of the Criminal Code)

This offence is committed by those who, for illicit gain, sell, receive, transport, export, import or, in any event, wrongfully manage significant quantities of waste. These shall not include sporadic events, but continuous activities for which proper means and organisation have been put in place. Highly radioactive substances shall constitute an aggravating circumstance.

False declaration on the origin of waste for SISTRI (article 260-*bis*, sub-article 6 – sub-article 7, 2nd and 3rd part - sub-article 8, EPP)[85]

Producers of waste and other persons involved in its management (sellers, brokers, collection or recycling consortia, persons undertaking collection or disposal operations) must participate or volunteer to participate in the IT system of control on the origin of waste known as SISTRI, according to criteria in Article 188-*ter* of the EPP. In this respect, offences consisting in providing false information on the nature and characteristics of waste in order to obtain a waste analysis certificate

[84] Article 4 of Legislative Decree 116/2020 reformulated Article 258 of the EPP starting from 26 September 2020, with the consequence that the second part of paragraph four, which still refers to Article 25-undecies of Legislative Decree 231/2001 provides for a different case, concerning the transport of hazardous waste without waste disposal records, while the offence described herein is now in the third part of the same paragraph. It is therefore considered that due to the oversight of the legislator, it can be argued that neither the new nor the original crime could constitute a predicate offence.

[85]. As from 1.1.2019, the waste disposal management register SISTRI has been abolished by Article 6 of Law Decree 135/2018, which has introduced a new waste traceability system, better defined in Legislative Decree 116/2020 (REN), with implementing provisions still to be completed..

to be entered in SISTRI, entering a false certificate in the system and using such certificate for the transportation of waste shall also be punishable.
The transport operator that uses a fraudulent hard copy of a SISTRI form, filled in for shipment of waste, is also punishable.

Breach of the regulations governing atmospheric emissions (article 279, sub-article 5, EPP)
This regulation punishes emissions into the atmosphere resulting from factory operations which exceed the limits established by law or as fixed in the licenses or regulations issued by the competent authorities and when they exceed the limits prescribed to ensure good quality of air in terms of current regulations.

Breach of regulations governing sale and detention of animals or plants which are in extinction or of dangerous mammals or reptiles (Law 150/1992, article 1, sub-articles 1 and 2 – article 2, sub-articles 1 and 2 – article 3-bis sub-article 1 - article 6, sub-article 4)
Offences consist in the import, export, transport and retention of animals and plants in breach of Community and international regulations which prescribe special permits, licenses and customs certificates, and false declarations or alteration of the above documents. The detention of certain dangerous mammals and reptiles is likewise prohibited.

Substances detrimental to the ozone layer (Law 549/1993, article 3, sub-article 6)
The law prohibits trade, use, import, export and retention of substances which are detrimental to the ozone layer as listed in the same law.

Pollution from ships (Legislative Decree 202/2007, articles 8 and 9)
Save as otherwise provided, this rule forbids commanders of ships, members of the crew, owners and ship builders from wilfully or negligently pouring into the sea hydrocarbons or harmful liquid substances transported in an improper manner.

7.12.2 Sensitive company activities

With reference to banking activities, the risk of committing offences against the environment could most likely arise in relationships with customers, with respect to granting loans or providing services in favour of persons involved in the illegal activities in question.
We cannot, however, exclude risks of directly committing illegal deeds concerning the production of waste, discharges, atmospheric emissions and ground pollution.

The protocol which lists the monitoring criteria and conduct criteria applicable to environment risk management is seen hereunder. This protocol is supplemented by company regulations which govern these activities.

Reference is also made to the protocols provided for in:

- paragraph 7.2.2.3. ("*Management of activities connected with the application for authorisation or the implementation of obligations vis-à-vis the Public Administration*")
- paragraph 7.2.2.8 ("*Management of the procedures regulating the provision of goods and services and professional appointments*")

which include principles of control and conduct aimed at avoiding offences defined in this paragraph.

Such protocols also apply to the monitoring of any activities performed by Group companies or outsourcers on the basis of special service agreements.

7.12.2.1. Environmental risk management

Introduction

This protocol applies to all the Bank's Structures involved in environment risk management.
In compliance with its Code of Ethics which identifies protection of the environment as a key value, the Intesa San Paolo Group has adopted a specific environmental and energy policy, which must be disseminated, understood and adopted at all levels of the organisation.

The Bank has adopted and maintains an Environmental and Energy Management System, which is verified annually by an international Certification Body, conforming to applicable laws and the most up-to-date reference standards: UNI EN ISO 14001 and UNI CEI EN ISO 50001.
The company has adopted a system of functions appropriate to the nature and size of the organisation and type of activity carried out, ensuring the necessary technical competences and powers for risk verification, assessment, management and control.

The corporate Structures in charge of managing environmental documentation, including authorisations and certifications issued by the Public Administration, must comply with the rules of conduct set out and described in the protocol "*Management of activities relating to applications or the fulfilment of requirements with the Public Administration*".

The definitions given in this protocol are aimed at ensuring the Bank's compliance with applicable regulations and principles of transparency, correctness, objectivity and traceability in carrying out the activities concerned.

Process description

With respect to environment risk, reference is made to the following processes:
Management of real estate and logistics:

- Territorial planning
- Management and maintenance of real estate in the territory;
- Planning of works;
- Execution of works.

Management of legal obligations governing waste:

- Waste management.

Management of expenses and purchases:

- Purchase cycle;
- Delivery management;
- “sourcing”.

Credit Management:

- Customer rating;
- special financing transactions;
- finance leases.

With specific reference to finance leases for real estate and/or moveable property, the Bank checks the conformity of said to environmental regulations, at the time of purchase and granting to customers, and also at the time of repossession, re-use, resale or disposal following the end of leasing for any reason whatsoever.
Procedures to manage and control the process are based on a clear, formalised assignment of duties and responsibilities with reference to the Structures involved (including external outsourcers) in controls on compliance with environmental regulations in force from time to time, and on a consistent system of authority, that governs the functions and powers arising from environmental regulatory obligations (Legislative Decree 152/2006).

The operating terms for management of these processes are governed by internal regulations, developed and updated by the competent Structures, which constitute an integral and essential part of this protocol.

Control principles

The control system for monitoring the processes described above must be based on the following elements:

- Authorisation levels defined within the process:
  - With respect to the purchase of goods and services, approval of the purchase request, appointment, signature of the agreement and issuing of orders shall be undertaken exclusively by persons duly empowered in terms of the system regulating assignment of powers and appointments in force which establishes the individual management powers by nature of expense and duty involved. The internal set of rules illustrates these authorisation mechanisms, and indicates the corporate officials who hold the necessary powers;
  - All transportation of special waste must be accompanied by an identification form signed by the transport operator and, as far as the Bank is concerned, by persons duly appointed for this purpose;

- Assignment to third parties - by suppliers of the Bank - of sub-contracted activities is contractually subject to the prior approval of the Bank structure which has stipulated the agreement and in compliance with the specific obligations in fulfilment of environment regulations.

- Separation of duties amongst the different persons involved in the environment risk management process. Specifically:
  - The operating Structures which are responsible for creating and managing activities involving services to individuals, buildings, maintenance, building and plant installation projects and other integrated services (e.g. toner supply, management of dispensaries, management of distributed IT equipment, controls/reconditioning/disposal of IT materials or products, etc.) are separate and distinct from the Structures responsible for consultancy on the evaluation of environmental risks and on monitoring the measures suited to prevent and limit them;
  - With respect to financing and advisory operations in Project Finance governed by the Equator Principles, the Structures responsible to ensure compliance with the applicable Equator Principles and the risks connected to social and environment matters are different from those responsible for the initial phase.

- Control activities:
  - The register identifying special waste duly filled in and signed by the transport operator must be checked by the person responsible within the Bank;
  - Sample checks on proper management of waste particularly special waste and, if present, hazardous waste carried out by the competent structures;
  - Review of the proper management of waste by the contractor resulting from ordinary and extraordinary maintenance and from building restructuring. More specifically, the contractor is bound to retrieve all "refuse" accumulated during its work cycle and the Managers or persons duly appointed by the Operating Units where the works are carried out must inspect that the contractors have properly performed their duties ensuring that no waste products are left within the Bank premises;
  - monitoring the proper implementation, by suppliers, of maintenance/cleaning services (for buildings and persons, etc.) with particular attention to the proper upkeep of maintenance logs for climate control systems, as well as regular maintenance reports drawn up by suppliers to whom said services have been subcontracted (e.g. reports on "leakage test" of reservoirs for storage of fuel);
  - with respect to financing and advisory transactions pertaining to Project Finance regulated by the Equator Principles, the product desk and/or relations function must regularly check compliance with environment requirements and, where necessary, propose corrective measures;
  - the competent structures delegated and/or identified by the Environmental Supervisor and Client must check:

- that the real estate and/or movable property to purchase to assign through finance leases are in conditions that ensure they conform to applicable regulations, checking that required conformity statements and documentation required by law have been provided;
- that in cases of the repossession of real estate and/or moveable property, or where information is obtained concerning possible user violations of environmental regulations, all related actions, also of a legal nature, functional to managing occupational environmental risks, also during the regular repayment of finance lease agreements, are carried out diligently and in adequate times;
- that the repossessed real estate and/or moveable property have been assessed for exposure to environmental risk (for example in the case of environmental pollution due to spills of hazardous or toxic waste) and actions to make them safe and clean-up actions have been planned.

- Process traceability including both the electronic and the paper trail:
  - use of IT systems supporting the operations, to ensure that the data and information relating to the procurement process are recorded and kept on file;
  - documenting all activities related to the process with particular reference to the proper upkeep and maintenance logs for climate control systems, in compliance with provisions of applicable legislation, particularly regarding emissions;
  - Preservation, as prescribed by law, (five years from last registration) of the register showing special waste (three years from the date of issue) and loading and unloading of hazardous waste for the three years following the date of the last registration;
  - In order to allow a clear understanding of the responsibilities and the motives behind the choices made, the Structure from time to time involved shall be responsible for archiving and preserving the documentation produced also by electronic means, in relation to the execution of the duties fulfilled in compliance with the above described processes.

Rules of Conduct

The Bank Structures, under whatsoever title involved in environment risk management, which is the subject of this protocol, as well as all the employees, are bound to observe the terms provided in this protocol, the legal provisions governing this sector and the internal regulations together with the provisions of the Group's Code of Ethics and Internal Code of Conduct.

In particular, all Structures shall - in their relevant fields:

- Monitor, for matters within their purview, the observance of environment regulations, particularly compliance with operating rules on the regrouping and temporary deposit of waste in compliance with its classification, on delivery to authorized, shippers, on the retention according to law of administrative documentation (Waste Identification Registers and, where applicable, the Loading and Unloading Register);

- monitor, for matters within their responsibility, compliance with environmental obligations, in particular on the management of boilers/heating systems, cooling units/heat pumps and emergency system electricity production plants;
- request the issue of declarations of conformity of owners, required by law, for the leased real estate and/or moveable property;
- Refrain from granting appointments/assignment of work to external consultants and/or suppliers in breach of the documented criteria and objectives aimed at ensuring professionalism and expertise, competitiveness, price, integrity and ability to guarantee an efficient assistance. More specifically the rules must be based on clarity and documentation in compliance with the Code of Ethics and the internal Code of Conduct of the Group;
- In the event that the involvement of third parties is envisaged for the management/prevention of risks, the agreements with these third parties must include a declaration of awareness of the regulations set under Legislative Decree 231/2001 and an undertaking to comply therewith;
- include, in supply, work and Service Supply Agreements for People, Building maintenance, building/plant works and other integrated services (e.g. toner supply, management of dispensaries, management of distributed IT equipment, controls/reconditioning/disposal of IT materials or products, etc.), specific clauses on compliance with environmental regulations;
- In terms of the purchase procedures applicable to products, machinery and tools, which at the end of their life cycle could be classified as potentially hazardous to the environment, the contracting Structures and the competent purchasing function must first obtain the "product hazard classification/material safety datasheet" and the EWR codes"[86], and all information necessary for correct disposal. In the case of purchases for leasing, the monitoring safeguards considered necessary based on the hazardous nature of the financed assets are adopted.
- Consider environment certifications as a vital requisite for evaluating the supplier, where the nature of the supply makes this possible and opportune;
- Consider the risk to the environment in evaluating credit rating, and in the case of customers belonging to sectors which are more at risk, obtaining specific information and supporting evidence;
- Adopting a transparent and collaborative stance with respect to controlling Entities (e.g. The Social Security Department (ASL), The Fire Department, ARPA, The Municipal Authorities, The Province Authorities, etc.) in the event of checks/inspections.

Likewise all employees shall:

- Comply with legal provisions and internal regulations and directives given by the company's Structures and the competent Authorities;
- Immediately notify the Manager and/or person responsible for emergency management of any environmental emergency (e.g. spillage of fuel, serious malfunction of equipment which could cause external noise beyond the approved limits).

[86] EWR - European Waste Register

In any event, it is forbidden to initiate, cooperate/give rise to conduct that could be considered an offence in terms of Legislative Decree 231/2001, and, more specifically by mere way of example, to:

- provide incomplete documentation and/or communicate false or modified data;
- use deceit which could lead Public Entities into error;
- deposit waste outside the "Temporary Landfill" and hand over special waste, as defined in the current internal regulations, to suppliers appointed to transport the same which are not included in the list of Companies authorised to manage waste available on the company intranet or to unauthorised operators in the event of waste from finance leases;
- authorise the purchase, or in any case authorise the financial leasing of real estate or and/or moveable property that do not conform to legal provisions and regulations in force;
- authorise the sale or a new lease for real estate and/or moveable property through finance leases that do not conform to legal provisions and regulations in force, save for any exceptions limited to cases where the asset is sold to a professional (supplier with proven knowledge and experience, authorised dealer, etc.), relieving Intesa Sanpaolo S.p.A. of all legal liability.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.13 Sensitive area concerning tax crimes

7.13.1 Type of offence

Introduction

The liability of entities is extended to some of the offences relating to income tax and value added tax provided for by Legislative Decree 74/2000, which sets out general rules on tax crimes, in order to strengthen the repression of the phenomenon of tax evasion and to implement the provisions of European legislation aimed at protecting the interests of the public finance of the Union.

New tax crimes have been included in Article 25-*quinquiesdecies*[87]. The offences in question are described below.

Fraudulent statement through the use of invoices or other documents for non-existent transactions (Article 2, Legislative Decree 74/2000)

Fraudulent statement through other artifices (Article 3, Legislative Decree 74/2000)

The first offence is committed by entities that file income tax or VAT tax returns that indicate fictitious payable items, resulting from invoices or other documents recorded in mandatory accounts or kept as evidence. The invoices or documents used refer to material falsification or provision of intentionally false statements concerning all or part of the transactions indicated, or regarding the counterparty.

The second crime exists if, apart from the use of invoices or documents certifying non-existent transactions as above, one of the aforesaid returns indicates amounts receivable below actual amounts, or fictitious payable amounts, receivables and withheld amounts, through transactions that are objectively or subjectively simulated, or using false documents, recorded in mandatory accounts or kept as evidence, or misrepresenting accounting, obstructing assessments or misleading the Tax Authorities. This crime does not exist if certain thresholds are not exceeded, or the misrepresentation is not attained through artifice, but simply due to the omission of invoicing and registration obligations, or by only indicating in returns items receivable which are below actual amounts receivable.

[87] Legislation on tax crimes was reformed by Legislative Decree 124/2019, of which Article 39 introduced tax crimes to Legislative Decree 231/2001, with effect from 24 December 2019. Article 5 of Legislative Decree 75/2020 then added the crimes of omitted or untrue statements and undue compensation, and made punishable - by amending Article 6 of Legislative Decree 74 / 2000 - the declaratory crimes referred to in Articles 2, 3 and 4 only if attempted, with effect from 30 July 2020.

Both crimes are committed with the presentation of statements. However, attempted crimes[88] are also punished, pursuant to Article 6 of Legislative Decree 74/2000, if preparatory acts are carried out for the fraudulent declaration, which may consist, for example, in the sole annotation of untrue information in the accounts, in order to evade VAT for a value of not less than €10 million and the facts occur partly in Italy and partly in another EU country.

Inaccurate tax return (Article 4 of Legislative Decree 74/2000)

Omitted tax return (Article 5 of Legislative Decree 74/2000)

Undue compensation (Article 10-quater of Legislative Decree 74/2000)

These offences punish those who:

- in annual VAT returns indicate assets for an amount below the actual amount, or non-existent liabilities, and certain thresholds of criminal relevance have been exceeded;
- do not file, and have the obligation to do so, a return relating to such taxes (or the return of the withholding agent) when a certain tax threshold has been exceeded;
- do not pay taxes due using unpaid credits as compensation, for an annual amount exceeding a certain threshold.

Such conduct also entails administrative liability pursuant to Legislative Decree 231/2001 only if it concerns the evasion of VAT for an amount not less than €10 million and if it is committed in the context of cross-border fraudulent systems.

In the presence of both circumstances, the crime of an inaccurate tax return is punished, pursuant to Article 6 of Legislative Decree 74/2000, even if it is only attempted[89] , that is, when there are preparatory acts, such as the omission of invoicing obligations, which may therefore have an effect on the subsequent tax return, if these facts are also carried out in the territory of another EU Member State.

Issue of invoices or other documents for non-existent transactions (Article 8, Legislative Decree 74/2000)

Subjects that, in order to enable third parties to evade income taxes or VAT, issue or provide invoices of other documents for non-existent transactions, commit a crime.

The subject issuing invoices or documents and party committing this crime cannot be punished for aiding and abetting a fraudulent statement of the third party that uses such documents, and similarly the third party cannot be punished for aiding and abetting the crime of issuing the invoices or documents.

[88] Pursuant to Article 26 of Legislative Decree 231/2001, the liability of entities for attempted crimes does not exist if the entity voluntarily prevents the completion of the action or the occurrence of the event.

[89] See previous note

Concealment or destruction of accounting documents (Article 10, Legislative Decree 74/2000)

This crime is committed by anyone who, in order to evade income taxes or VAT or that enables third parties to evade, conceals or destroys in whole or in part accounting records or documents which must be retained, so as to prevent the reconstruction of income or business turnover.

Fraudulent omission of tax payments (Article 11, Legislative Decree 74/2000)

The punished conduct involves carrying out simulated or fraudulent acts on own or third-party property, which can invalidate the procedure to collect income tax and VAT, interest or administrative fines relative to such taxes, for a total amount of more than 50 thousand euro.

The conduct of anyone who, as part of a tax transaction, in order to obtain for themselves or others the reduced payment of taxes and additional items, indicates in filed documents amounts receivable that are lower than actual amounts or fictitious payable amounts for a total amount of more than 50 thousand euro, will also be punished.

7.13.2 Sensitive company activities

The risk of committing tax crimes is possible in all company activities. It is specifically governed by the protocol "Management of risks and obligations for the prevention of tax crimes".

As regards the Bank's position as taxpayer, this risk is also governed by the protocol "Management of periodic reporting". The following should also be considered:

- the Bank has joined the cooperative compliance scheme with the Tax Authorities contemplated in Article 3 of Legislative Decree 128/2015 and has adopted for this purpose a system to identify, measure, manage and control tax risk, described in the "Guidelines to manage tax risk in the cooperative compliance scheme with the Tax Authorities" and in other sources of detailed company regulations;
- since 1 January 2019, the Bank has opted to set up a VAT Group, as regulated by Part V-bis of Presidential Decree 633 and the relative implementing decree Ministerial Decree of 6 April 2018. Participation in a VAT Group entails a single (new) tax entity being set up, as the VAT Group: i) has a single VAT number, ii) operates as a single VAT taxable subject in relations with entities not belonging to the group, iii) fulfils all obligations and exercises all relevant rights/options (e.g. separation of activities for VAT purposes) for VAT purposes. The IVA group operates through the representative company (Intesa Sanpaolo) which exercises control over the other participating companies[90] ;
- the Bank has activated, starting from 2004, the National Tax Consolidation, governed by Articles 117-129 of the Consolidated Income Tax Act, which almost all resident companies of the Intesa

[90] The regulation requires the mandatory participation ("all-in all-out" clause) of all subjects bound by financial, economic and organisational constraints with the Parent Company.

Sanpaolo Group are party to, on an optional three-year (renewable) basis. As a result of the aforementioned option, each company, including the consolidating company, continues to autonomously declare its income or tax loss, in addition to withholding taxes, deductions and tax credits; these components are understood to be transferred by law to the parent/consolidating company which, in the context of the consolidated tax return (CNM model) (i) determines a single taxable income or a single tax loss that can be carried forward resulting from the algebraic sum of own income/losses and of the consolidated companies, (ii) makes the consolidation adjustments required by law, (iii) deducts the withholdings and own tax credits and those transferred from the consolidated companies, to determine the single IRES payable or credit pertaining to the Tax Consolidation.

As regards relations with third parties, such as customers, suppliers, partners and counterparties in general in order to mitigate the risk of being involved in tax crimes, also in view of the fact that the law, pursuant to Article 13 bis of Legislative Decree 74/2000, severely punishes banking and financial intermediaries that take part in the processing or marketing of tax evasion models, the Bank has also prepared protocols regulating the following activities:

- Management of the procedures for the procurement of goods and services and for the appointment of professional consultants;
- Management of gifts, entertainment expenses, donations to charities and sponsorships;
- Management of real-estate and cultural assets;
- Purchase, management and disposal of investments and other assets;
- Financial fight against terrorism and money laundering;

that contain the principles of control and conduct to observe also for the purposes of preventing tax crimes.

With reference to the management of tax risk relative to products and services offered to the customer, which concern cases where the Bank could be potentially involved in irregular tax transactions of customers, the regulations in the “Guidelines for the approval of new products, services and activities intended for a certain customer target", in the “Rules for evaluating the tax conformity of products of services and transactions proposed to customers” and in the internal regulations on credit management apply.

It cannot be ruled out that the violation of the obligations of notifying the Revenue Agency of the cross-border mechanisms provided for by Legislative Decree 100/2020, beyond the specific administrative sanctions envisaged, can be interpreted as an indication of a previous involvement of the bank's appointee in the customer’s fiscal/tax violations, violations which, in this context, in reference to the known conditions of interest or advantage, could, where attributable to predicate offences (of both a both fiscal and money laundering/self-laundering nature), entail liability risks for the Bank pursuant to Legislative Decree 231/2001. In this regard, Group Rules for the management of the reporting obligations envisaged by DAC 6 (“Directive on Administrative Co-operation”) establish the roles and responsibilities in managing the process to identify and report operations.

Such protocols also apply to the monitoring of any activities performed by Group companies or outsourcers on the basis of special service agreements.

7.13.2.1. Management of risks and obligations for the purposes of preventing tax crimes

Introduction

This protocol applies to all Bank structures involved in managing risks and obligations for the purposes of preventing tax crimes.

Pursuant to Legislative Decree 231/2001, the process could pose risks of the following tax crimes being committed: *"Fraudulent statement through the use of invoices or other documents for non-existent transactions", "Fraudulent statement through other artifices", "Issue of invoices or other documents for non-existent transactions", "Concealment or destruction of accounting documents " and "Fraudulent omission of tax payments", "Inaccurate tax return" "Omitted tax return", "Undue compensation".*

Moreover, company rules and controls on completeness and truthfulness in this protocol are also prepared in order to enhance actions to prevent crimes that could result in the incorrect management of financial resources, such as "*Money laundering*" and "*Self-laundering*".

As established in "Principles of conduct on taxation", Intesa Sanpaolo and its Group intend maintaining cooperative, transparent relations with the Tax Authorities and promoting participation in cooperative compliance schemes.

The definitions given in this protocol are aimed at ensuring the Bank's compliance with applicable regulations and principles of transparency, correctness, objectivity and traceability in carrying out the activities concerned.

Process description

The process to manage risks and obligations for preventing tax crimes address, directly and/or indirectly, a diverse number of company processes that concern:

- the purchase and sale of goods and services;
- the representation of operations in accounts and company systems;
- the management of obligations concerning invoices payable and receivable, and those relative to the "VAT Group";
- the preparation of tax returns and the correct payment of relative taxes;
- the obligations related to the "Cooperative compliance scheme with the Tax Authorities", which the Bank is party to.

The representation of operations in the accounts and company systems, including the evaluation of individual items, is governed by the protocol "*Management of periodic reporting"*.

Relations with the Tax Regulators (Tax Authorities) are governed by operating rules set out in internal regulations to manage relations with the Regulators and in the protocol "*Management of relations with the Supervisory Authorities*".

The operating procedures for management of the processes are governed by the internal rules, which are developed and updated by the competent Structures, and which form an integral and substantive part of this protocol.

Control principles

The control system for monitoring the processes described above must be based on the following elements:

- Authorisation levels defined within the process:
  - all subjects involved in managing activities concerning the preparation of tax returns, and in activities relating to the issue / registration of invoices: are identified and authorised according to the specific role assigned by the organisational code or by the Head of the reference Structure by means of internal delegation, to be kept on file by the same Structure;
  - if external consultants/suppliers are involved, they are identified in a letter of appointment, or in contract clauses; only operate within the scope assigned to them by the Head of the reference Structure;
  - each agreement/contract with the Tax Authorities is formalised in a document, duly signed by subjects with suitable powers based on the system of powers and authority adopted;
  - in cases where the tax strategy the Bank intends adopting is not agreed by the Tax Authorities, final adoption must be approved by the Board of Directors, after an assessment by the Head of the Tax Function on the risks and costs/benefits arising from the position the Bank wishes to adopt and after an opinion from at least one high-standing external tax consultant.

- Segregation of duties among different persons involved in processes to manage risks and obligations for the purposes of preventing tax crimes. Specifically:
  - the activities relating to the different phases of the process must be carried out by different and clearly identifiable persons, and must be supported by a maker and checker mechanism.

- Control activities:
  - the controls concerning the completeness, correctness and accuracy of the information provided to the tax authorities by the Structure concerned as to the activities falling under its competence that must be supported by maker and checker mechanisms;
  - legal controls on compliance with legislation applicable to tax returns;
  - automated ongoing system controls concerning periodic tax returns;

- controls on the correct issue, adoption of VAT rates and registration of invoices receivables and their correspondence with contracts and undertakings with third parties, including finance lease arrangements (surrender by the lessor, sale to third parties of the repossessed good);
- objective and subjective controls on the actual underlying relationship with invoices payable received and on correct registration and accounting, including finance lease arrangements (purchase by the Bank for subsequent profit realisation).

- Process traceability including both the electronic and the paper trail:
  - each significant phase of the risk management process and obligations for the purposes of preventing tax crimes must be recorded in written documentation;
  - in order to reconstruct the responsibilities and reasons for choices made, each structure is in charge of filing and retaining competent documents produced digitally or electronically.

- Bonus or incentive systems: bonus and incentive systems must be able to guarantee compliance with legal provisions, the principles of this protocol and the provisions of the Code of Ethics, also envisaging suitable corrective mechanisms for any conduct deviating from the norm.

Rules of Conduct

The Bank Structures, involved for any reason in managing risks and obligations for the purposes of preventing tax crimes covered by the protocol, are required - like all employees - to observe the procedures indicated in the protocol, applicable legal provisions, internal regulations as well as requirements of the Group's Code of Ethics, Internal Code of Conduct, Administrative/Financial Governance Guidelines, Principles of Conduct on Taxation and Guidelines for managing tax risk in the cooperative compliance scheme with the Tax Authorities. In particular, all Structures shall - in their relevant fields:

- guarantee the true and fair representation of financial data in the Bank's tax returns;
- comply with principles of conduct on taxation, in order to: (i) guarantee conformity over time to the tax legislation of countries where the Bank operates and, (ii) the financial integrity and reputation of all Group Companies;
- act based on values of honesty and integrity in managing the tax variable, aware that income from taxes constitutes one of the main sources that contributes to the economic and social development of countries where they operate;
- guarantee the fostering of a company culture based on values of honesty and integrity and the principle of lawfulness;
- maintain cooperative, transparent relations with the Tax Authorities, guaranteeing that the Authorities have a full understanding of facts behind the adoption of tax regulations;
- meet tax obligations according to the times and procedures defined by regulations or the tax authorities;
- avoid types of tax planning that may be considered as aggressive by the tax authorities;

- interpret regulations according to their intent and purpose, without any exploitation of their literal formulation;
- represent acts, facts and negotiations undertaken in such as way that applicable tax regimes may be applied that conform to the actual economic substance of the transactions;
- guarantee the transparency of operations and the determination of income and assets, avoiding the use of structures, also corporate, that may conceal the actual beneficiary of the income flows or ultimate owner of the assets;
- respect provisions that can guarantee suitable transfer pricing for intergroup transactions with the purpose of allocating generated income in compliance with law;
- assist competent authorities in order to provide complete, truthful information necessary for tax obligations and controls;
- establish cooperative relations with the tax authorities, based on transparency and reciprocal trust and aimed at preventing conflict, limiting disputes as far as possible;
- propose products and services to customers that do not make it possible to unduly have tax benefits that could not otherwise be obtained, through adopting appropriate safeguards to avoid involvement in improper tax transactions of customers.

In any event, it is forbidden to initiate, cooperate/give rise to conduct that could be considered an offence in terms of Legislative Decree 231/2001, and, more specifically by mere way of example, to:

- provide incomplete documentation and/or communicate false or modified data;
- adopt deceitful conduct which might lead the Tax Authorities into error;
- pay an invoice without checking the actual existence, quality, suitability and prompt nature of the service received, and that the counterparty has met all obligations;
- use false structures or companies, not related to the business activity, solely for the purpose of tax evasion;
- issue invoices or other documents for non-existent transactions in order to enable third parties to evade taxation;
- indicate in annual income tax and VAT returns: i) fictitious payable items, using invoices or other documents which are equivalent, in terms of evidence, to invoices, for non-existent transactions; ii) items receivable for an amount lower than the actual amount or fictitious payable items (for example costs fictitiously incurred and/or revenues indicated that are lower than the actual amount) referring to a false entry in mandatory accounting records and using means suitable for obstructing assessment; iii) a taxable base of a lower amount than the actual amount, by presenting items receivable for an amount lower than the actual amount or fictitious items payable; iv) apply, without reason, the terms of applicable legislation for presenting items, and for subsequent payment of resulting taxes.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

APPENDIX: Bribery act

The Bribery Act entered into force in the United Kingdom on 1 July 2011. This Act modified and supplemented the pre-existing legislation governing corruption, introducing, inter alia, a new liability upon entities for cases of corruption in their favour or in their interest, where such entities do not have in place adequate internal procedures to prevent said offences.

More specifically, English law set forth a homogeneous set of regulations governing corruption, based on four main types of offence:

- The first relates to the offer, the promise or the grant to others of financial or other type of advantage in order to obtain or compensate the illegal execution of activities or services falling within their purview of control or responsibility or that of third parties (the purview of activities are defined in the law both in the public sector as well as for private professional and commercial activities);
- The second type consists in requesting, receiving or accepting to receive such advantage (an attempt is also punishable);
- The third case concerns the crime of "*Corruption of a foreign public official*", extending application of relevant provisions to outside the United Kingdom;
- The fourth case is the "corporate offence" which consists of failure by the commercial company to adopt suitable measures to prevent corruption by "associated persons", which include persons who provide a service in the name and on behalf of the company, irrespective of the nature of the relationship between the person and the company. In cases where the person is an employee, unless evidence to the contrary is given, the person is presumed to be an associated person.

With particular reference to the last type of offence (Failure of commercial organizations to prevent bribery) it must be pointed out as follows:

- Bodies which do not carry out activities which fall under "business" are excluded;
- Only the conduct of the "associated person" is taken into consideration for the existence of the liability of the entity;
- The liability of the entity exists only if the associated person is guilty of an offence in terms of the Bribery Act (corruption of a private individual or of a public official);
- The entity could be exempt from liability if it proves to have adopted, prior to the offence, "adequate procedures" aimed at preventing corruption.

The Bribery Act provides that entities responsible for corporate offences shall be punishable by unlimited fines, while the persons committing the offence of corruption shall be subject to fines and imprisonment.

The Bribery Act is relevant to Italian companies insofar as it applies to all companies (whether British or not) which exercise their activities or part thereof in the United Kingdom.

Therefore, the Bank Structures, as well as all employees and those who carry out a service in the name and on behalf of the Bank and who work with British counterparts or, in any event, in the United Kingdom, besides respect for the provisions of the Code of Ethics, the Group Internal Code of Conduct, the Group Anti-corruption Guidelines and this “Organisational, management and control model", must also abide by the provisions of the Bribery Act and pro tempore internal regulations applicable to the London Branch in this respect (particularly the Intesa Sanpaolo Anti-Bribery & Corruption policy available at the Bank document repository).