ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL

Pursuant to Legislative Decree no. 231 of 8 June 2001

Approved by the Board of Directors on 4 February 2019

BANCA IMI

TABLE OF CONTENTS

Chapter 1 – The regulatory framework

1.1 The administrative liability scheme laid down in Legislative Decree no. 231/01 for legal persons, companies and associations, including unincorporated associations

By way of implementation of the delegation under Article 11 of Law No 300 of 29 September 2000, on 8 June 2001 Legislative Decree no. 231 (hereinafter the "Decree" or "Legislative Decree no. 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 Communities' financial interests of 26 July 1995, the Brussels Convention on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union, signed 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.) for a series of specified criminal /administrative offences committed 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 was the perpetrator of the offence, and is independent of it, as it also exists where the perpetrator 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, interdictions, confiscation, publication of the sentence and appointment of a special administrator. Interdiction 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 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 criminal/administrative 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 organisational, management and control models 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 models, and with updating the model.

The *Organisational, Management and Control Model pursuant to Italian Legislative Decree no. 231 of 8 June 2001* (hereinafter also the "Model") must meet the following requirements:

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

If the criminal/administrative 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: (i) management had adopted and effectively implemented an appropriate Model to prevent criminal/administrative offences of the

kind that has occurred; (ii) the task of monitoring Model implementation, compliance and updating was entrusted to a corporate body with independent powers of initiative and control; (iii) the perpetrators committed the criminal/administrative offence by fraudulently circumventing the Model; (iv) there was no omission or insufficient control by the control body.

On the other hand, where the criminal/administrative 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 criminal/administrative offence was made possible by non-performance of management and supervisory duties. Such non-performance shall be ruled out where the entity, before the criminal/administrative offence was committed, had adopted and effectively implemented an appropriate Model to prevent criminal/administrative 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 Banca IMI S.p.A. (hereinafter also referred to as “the Bank”) was prepared and updated – in view of the specific nature of the Bank’s business and organisational structure - in compliance with the principles and contents of the Model of the Parent Company Intesa Sanpaolo S.p.A. (hereinafter also referred to as “the Parent Company”), and with the Guidelines prepared by ABI and ASSOSIM, approved by the Ministry of Justice.

Chapter 2 - The Organisational, Management and Control Model pursuant to legislative decree no. 231 of 8 June 2001 of Banca IMI S.p.A.

2.1 The existing corporate tools underlying the Model

In preparing this Model, account was taken firstly of the current legislation and of the procedures and control systems already existing and implemented within Banca IMI 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 no. 231/01.

Banca IMI S.p.A. is a highly complex reality, from both the organisational and operational viewpoint.

The corporate bodies of Banca IMI S.p.A. have given the highest importance to aligning organisational structures and operational procedures with the Parent Company's directives, 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 Banca IMI 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 Banca IMI S.p.A. as both a bank and a company belonging to the Intesa Sanpaolo banking group (Banking Law, the Consolidated Law on Financial Intermediation, etc.) and the consequent provisions issued by supervisory Authorities (the European Central Bank, the Bank of Italy, Italy's Securities Exchange Commission,[1] etc.) within their respective powers, which carry out checks and controls on the Bank's activities and organisational structure, as provided for by law.

The regulatory provisions also include the obligation for the Parent Company to draw up, pursuant to Legislative Decree no. 254/2016, a consolidated non-financial statement, which, to the extent necessary to ensure an understanding of the Intesa Sanpaolo Group's business, its performance, results and impact, covers environmental, social, personnel, human rights and anti-corruption issues. The Statement must describe the business model for the management and organisation of business activities, including the organisational, management and control

[1] Prudential Regulation Authority (PRA) e Financial Conduct Authority (FCA) as far as regards the London branch.

models adopted pursuant to Legislative Decree no. 231/2001, the policies applied with reference to the management of the above issues and the main inherent risks.

As a member of the Intesa Sanpaolo banking group, the Bank is also subject to the guidance, governance and support exercised and provided by the Parent Company and is bound to observe the provisions laid down by said Parent Company within the context of the governance of its own subsidiaries.

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 relevant corporate laws and regulations, and with the directives of the Parent Company;
- internal regulations and corporate policies;
- the Group's Code of Ethics, Internal Code of Conduct and Anti-Bribery 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 organisation, management and control system which all internal and external parties are required to respect, in accordance with their relationship with the Bank.

The Model is also completed by all the mandatory regulatory provisions set out by the sector's Supervisory Authority governing specific areas of the operations of Banca IMI S.p.A. (e.g. the Supervisory Instructions for banks issued by the Bank of Italy, CONSOB's Regulations, the Resolutions of the Inter-Ministerial Credit and Savings Committee (CICR – Comitato Interministeriale per il Credito ed il Risparmio), Market Rules, the Rules promulgated by the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA).

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

2.1.1 The Group's Code of Ethics, Internal Code of Conduct and Anti-Bribery 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 implements the Code of Ethics, the Internal Code of Conduct and the Anti-Bribery Guidelines adopted by Banca Sanpaolo S.p.A.

The Code of Ethics is a voluntary self-regulation tool, an integral part of the Corporate Social Responsibility management model. It contains the mission, corporate values and principles that govern relations with stakeholders, starting with the corporate identity. In certain areas of particular importance (e.g., human rights, labour protection, environmental protection, the fight against corruption), it makes reference 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, personnel 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.

In line with the international best practice, the Anti-Bribery Guidelines identify the principles, sensitive areas, roles and responsibilities, and macro-processes for the management of corruption risk by the Intesa Sanpaolo banking group. They also provide for assigning the responsibility for monitoring the matter to the Anti-Money Laundering function of the Parent Company and the role of Anti-Bribery Officer to its Manager for both Intesa Sanpaolo S.p.A. and for the companies for which the monitoring of compliance with the administrative liability of Entities is centralised in the Parent Company.

2.1.2 The key features of the internal control system

Banca IMI 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 instructions of the Parent Company, has adopted an internal control system capable of identifying, measuring and continuously monitoring the risks typical of its business activities.

Banca IMI 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 safeguard of asset value and protection from losses;
- 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 231/2001.

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 Regulation, Regulation on Related Party Transactions, Regulation of 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 (Policies, Process Guidelines, Operating Guidelines, Control Records, 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 univocally and formally identify responsibilities, 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:

- ***first tier:*** line controls designed to ensure that operations are carried out correctly and that, insofar as possible, these are incorporated into IT procedures, or through systematic and random manual controls; in the latter cases, these controls are performed by the operational

and business organisational units themselves, including through units that are exclusively dedicated to control tasks and that report to the heads of the units, or are performed as part of back-office and post-trading operations. The operational and business organisational units have the primary responsibility for the risk management process and must comply with the operational limits assigned to them in accordance with the risk objectives and the procedures underlying the Bank's risk management process;

- ***second tier***: controls on risks and compliance that aim to ensure, inter alia: (i) correct implementation of the risk management process; (ii) compliance with the operational limits assigned to the various functions; (iii) legal and self-regulatory compliance of business operations. The functions responsible for these controls are distinct from the production functions and contribute to defining the risk governance policies and the risk management process;
- ***third tier:*** internal auditing activities, designed to identify violations of procedures and regulations and to periodically assess the comprehensiveness, adequacy, functionality (in terms of efficiency and effectiveness) and reliability of the internal control system and the IT system, at pre-established intervals depending on the nature and severity of the risks. Third tier controls are carried out by different organisational units that are independent of production and second level functions.

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

  In particular, the system of internal controls reproduces the instruments and methods currently in use at Intesa. With the exception of the line controls and the hierarchical controls, overall operations are centralised under the Parent Company's control functions, provision obviously being made for suitable lines of reporting to the Bank's Administrative Bodies and senior management. Basically, the system of internal controls adopted by the Bank establishes that line controls are performed by the structures of Banca IMI S.p.A. as well as the responsible structures of the Parent Company; the management, assessment and monitoring of credit, financial and operating risks are outsourced to the Parent Company's structures; audit and compliance controls are centralised and performed by the Parent Company, acting in such capacity. This decision is supported by the guidelines contained in the supervisory provisions, which envisage the opportunity – within the context of the Group's strategies – to centralize the Internal Auditing and Compliance function at one of the banks within the Group.

2.1.3 The power 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, and has appointed a Managing Director, and a General Manager, granting them specific powers in accordance with the duties performed, setting any 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 always 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 personnel members jointly or severally, depending on whether the documents in question are binding on the Company vis-à-vis third parties, or whether they are simply designed to provide information.

All the Structures operate under specific Regulations defining their powers and responsibilities; these Regulations are issued and made public within 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 (Internal Circulars and Notes signed by persons vested with such powers).

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 criminal/administrative 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 criminal/administrative offences identified in the Decree), increasingly 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, in line with the Parent Company, 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 criminal/administrative 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 criminal/administrative 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;
  - the 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;
  - the appropriate procedures for performing the activities;
  - traceability of the acts, operations and transactions through an appropriate paper or electronic trail;
  - the presence of decision-making processes linked to pre-set objective criteria (e.g.: the company keeps registers of approved suppliers, objective personnel 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 Supervisory 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 Supervisory 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;
- personnel 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 no. 231 of 8 June 2001*," Banca IMI S.p.A. took as a basis, supplementing them, the internal rules and procedures already in place, on the basis of the mapping of sensitive areas and activities performed when the Model and its subsequent updates were adopted.

Accordingly, for each category of "predicate offence", the "sensitive" corporate areas have been identified. 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 risk of criminal/administrative offence to be prevented.
The Model is fully and effectively implemented in the Bank's operations by connecting each sensitive area with the corporate structures from time to time concerned 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 existing store of knowledge concerning the internal policies, rules and regulations guiding and governing the Bank's 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;
- makes it easier to regularly implement and update in a timely manner the internal processes and regulatory system, in response to changes in the company's organisational structure and operations, making the Model highly "dynamic".

Accordingly, the control of risks within Banca. under the system of liability introduced by Legislative Decree no. 231/2001, is guaranteed by:

- this document ("Organisational, Management and Control Model pursuant to legislative decree no. 231 of 8 June 2001");
- the existing regulatory system, which is an integral and substantive part of this Model.

The "*Organisational, Management and Control Model pursuant to legislative decree no. 231 of 8 June 2001*" 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 Supervisory Body;
- the information flows from and to the Supervisory Body;
- the system of sanctions;
- the training principles;
- the "sensitive" areas having regard to the types of offence 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, consisting of the "*Governance Documents*" (Articles of Association, Code of Ethics, Group Internal Code of Conduct, Guidelines, Regulations, Rules, Authorities, Function/Organisational Charts, etc.), Policies, Operating procedures, Process Manuals, Control Records 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 personnel of Banca IMI S.p.A. (including those recruited and/or working abroad) and, in particular, by those who perform sensitive activities.

Personnel training and the dissemination of information on Model contents within the organisation are constantly guaranteed by the procedures described in detail in Chapter 6 below.

In order to ensure the effective and efficient prevention of criminal/administrative offences, the Model is also addressed to external stakeholders (i.e. suppliers, agents, consultants, professionals, self-employed or "para-subordinate" workers, commercial partners, etc.) 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, under penalty of termination of the contract, to comply with the principles of the Model and Anti-corruption Guidelines and to report any case of unlawful acts or breaches of the Model they might become aware of to the Supervisory Body and Anti-Bribery Officer.

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 proposal from the Managing Director.

The **Managing Director** defines the structure of the Model to be submitted to the **Board of Directors**' approval with the assistance, as to their respective areas, of the Bank's Compliance, Internal Auditing, Anti-Money Laundering, Parent Company Corporate Advice and Affairs, Organisation and Personnel, and Legal Affairs functions, of the Employer, of the Principal pursuant to Legislative Decree no. 81/2008, and of the Environmental Affairs Officer pursuant to Legislative Decree no. 152/2006 after consultation with the Supervisory Body.

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 Supervisory 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 Supervisory Body, in 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 of the Bank and/or Parent Company, having regard to the activities at risk they perform.

The Board of Directors, also with the help of the Supervisory Body, must also ensure updating of the sensitive areas and of the Model, in view of any updating requirements which might become 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 monitoring of 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 directly supports the Supervisory 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 corrective 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 Supervisory Body's performance of its control activities by:

- defining and updating the Model, with the support of the Organisation functions, of the employer and of the Principal, pursuant to Legislative Decree no. 81/2008, of the Environmental Affairs Officer pursuant to Legislative Decree no. 152/2006 and of the Anti-Money Laundering function, insofar as each of them is concerned, in line with developments in the reference legislation and with changes in the organisational structure, and with the support of the Legal Affairs function of Intesa Sanpaolo as far as concerns the interpretation of the law, the settlement of legal questions and the identification of any conduct that could constitute a criminal offence;
- monitoring, on an ongoing basis, the effectiveness of the Model as regards the standards and rules of conduct for preventing serious 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 inexistence 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 hetero-regulating (regulatory laws and rules) and self-regulating codes on the subject of money laundering, terrorism financing, violation of embargoes, corruption and armaments, and administrative liability[2].

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, the violation of embargoes, and armaments:

- 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, an adequate training plan aimed at keeping employees and collaborators constantly updated.

Legal Affairs function

Banca IMI's General Counsel Affairs function, in cooperation with the appointed functions at Intesa Sanpaolo pursues the aims set out in the Decree by providing assistance and legal

[2] The tasks relating to the administrative liability of entities are described in this Model in the paragraph relating to the Compliance function

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 criminal/administrative offences.

The Legal Affairs function cooperates with Compliance, Internal Auditing and Organisation in updating the Model, also reporting any widening of the scope of the administrative liability of Entities.

Corporate Advice and Affairs function

The Corporate Advice and Affairs function, in keeping with its institutional role, is responsible both for guaranteeing advice and assistance with specific regard to the characteristics and activities of the Supervisory Body, and for reporting to the appointed Corporate Bodies, in the event of any corporate transactions or transactions of any other nature that modify the Company's operating framework, with regard to the need to modify the Model in order to take account of the new situation that has emerged.

Organisation function

In consultation with the respective functions of Intesa Sanpaolo, each within its own remit, in order to ensure that the organisational structure and governance mechanisms are in line with the objectives pursued by the Model, Banca IMI's Organisation function, shall:

- design the organisational structure, defining its missions, organisation charts and functions, to be submitted to the relevant Parent Company functions and Board of Directors for approval;
- set out the rules for the design, official adoption and management of the organisational processes, in line with the Parent Company's methods and instruments;
- 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 Supervisory Body;
- work with the Organisational units, the Internal Auditing, Compliance, Legal Affairs and Parent Company's Anti- Money Laundering functions, with the Employer, with the Principal, pursuant to Legislative Decree no. 152/2006, with the Environmental Affairs Officer pursuant to Legislative Decree no. 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.

Personnel function

Banca IMI's Personnel function, in keeping with its subordination to the Personnel Service of the Parent Company's CIB Division, as described in detail in Chapter 5 and Chapter 6:

- develops, supported by the Training function, training plans and awareness-raising actions, with support from the Training and Internal Communications and other competent functions, addressed to all personnel members concerning the importance of adhering to the company's rules of conduct, understanding the contents of the Model, Code of Ethics, Group Internal Code of Conduct and Group Anti-Bribery Guidelines, and specific courses addressed to the personnel operating in the sensitive areas, in order to clarify in detail issues, early warning signs of anomalies or irregularities and the corrective actions to be taken for anomalous or risk-exposed operations;
- manages, with support from the Internal Auditing, Compliance, 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; in turn, it reports all information collected concerning the facts and/or conduct relevant to compliance with the provisions of the Decree to the Supervisory 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 Supervisory 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, Principal pursuant to Legislative Decree no. 152/2006, Environmental Affairs Officer pursuant to Legislative Decree no. 152/2006

The parties identified as Employer and Principal pursuant to Legislative Decree no. 81/2008 and the Environmental Affairs Officer pursuant to Legislative Decree no. 152/2006, only as concerns their respective area of responsibility for managing the risks relating to workplace health and safety and to temporary and 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 organisational model of Banca IMI S.p.A. provides for the "outsourcing" of a part of Banca IMI S.p.A.'s control, administrative, middle office and back office activities, to the Parent Company, other Group Companies, and/or third-party outsourcers.

In particular, the Bank has assigned the operational management of some of the activities concerning real estate and procurement, organisation, process governance and development, security, operational services, information services, and internal communications to Intesa Sanpaolo and credit recovery services to a third-party outsourcer.

The outsourcing of said activities is carried out in accordance with the prescriptions of the competent Supervisory Authorities and is formalised through the conclusion of specific contracts that enable Banca IMI S.p.A. to:

- take all decisions in accordance with 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, said contracts include:

- a detailed description of the outsourced activities;
- the way in which the services are to be provided;
- specific service levels;
- the verification and control powers remaining with the Bank;
- the rates applying to the services rendered;
- appropriate reporting systems;
- appropriate safeguards protecting the Bank's information assets and transaction security;

- the obligation for the outsourced service provider to operate in accordance with the current laws and regulations and to ensure they are also complied with by any third parties he might avail himself of for performance of the outsourced activities;
- the possibility for Banca IMI S.p.A. to terminate the contract in the event it is breached by the service provider: (i) of the legislation and requirements issued by the Supervisory authorities which may involve sanctions for the principal; (ii) of the obligation to implement the activities in compliance with the principles laid down in the Model pursuant to Legislative Decree no. 231/2001 adopted by Banca IMI, the Code of Ethics, the Group Internal Code of Conduct and the Group Anti-Bribery 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 (the Parent Company and/or other Companies within the Group).
Outsourcing contracts do not govern performance of the Parent Company's institutional activities in such capacity, including those aimed at defining the strategic guidelines of the Group and of the companies within the Group, and designed to guarantee the uniformity of processes and actions.
As previously mentioned, as far as concerns the system of internal controls, in implementation of the option provided in regard thereof in the Bank of Italy's Supervisory Instructions, performance of the Internal Auditing, Compliance and Anti-Money Laundering functions has been centralised with the Parent Company.

2.8 The Parent Company's role

Without prejudice to the independent responsibility of each Banca IMI Group Company as regards the adoption and efficient implementation of its own Model in accordance with the Decree, in exercising its specific function as Parent Company, Intesa Sanpaolo has the power to establish criteria and guidelines of a general nature and to verify, through the Compliance, Internal Auditing and Corporate Advice and Affairs functions, whether the Group companies' Models 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 defined by the Parent Company, which all the companies incorporated in Italy, and thus also Banca IMI, 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, in the Group Internal Code of Conduct and in the Group Anti-Bribery 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 Supervisory Body, in line with the Parent Company's recommendations on the persons to be appointed.

  In the event that the members of the Supervisory Body do not coincide with those of the Control Body of the subsidiary, the Equity Investments function provides information to the Management Control Committee;
- 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;
- in collaboration with the Parent Company's Human Resources and Compliance functions and with support from the Training and Internal Communications functions, prepare training and communication activities addressed to the whole Personnel as well as specific training

targeting figures engaged in activities more sensitive to the Decree, so as 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, each year the company's Compliance function shall follow a risk-based approach to identify those processes felt to be at higher risk for the predicate offences, having regard to both their contents and to the existence or inexistence of specific risk-mitigating procedures. For such processes the Compliance function shall:
  - issue a preliminary approval, prior to their publication, concerning the sound application of the control and conduct principles provided for by the Model;
  - implement specific assurance activities to assess the conformity of the processes with the "protocols" set out in the Model;
- perform, 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 Risk Management and Compliance functions;
- submit to the Compliance function copy of the periodic reports, also including the results of the self-assessment exercise, submitted by the Compliance function to the Supervisory Body.

The company's Supervisory Body, through the Corporate Secretariat, shall also forward to the Chairman of the Parent Company's Management Control Committee 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.
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 Banca IMI, 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 Compliance function; nevertheless, the competence and responsibility to approve and effectively implement the Model and appoint the Supervisory Body shall remain with Banca IMI, together with 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 Compliance function a copy of the notices convening the meetings of the Supervisory Body and the meetings of the Corporate governance bodies whenever Decree-related issues are on the agenda.

Chapter 3 - The Supervisory Body

3.1 Identification of the Supervisory Body

In accordance with the Decree, the task of monitoring the Model's implementation, compliance and updating was entrusted to a specific body of the Entity with autonomous powers of initiative and control ("Supervisory Body").

The Supervisory Body must fully meet the requirements of autonomy, independence, professionalism and continuity of action necessary for the sound and efficient performance of those duties it has been assigned. It must also be provided with powers of initiative and control on the Company's activities and has no management or administrative powers.

Taking account of the provisions of paragraph 4-bis of Article 6 of Legislative Decree no. 231/01, as introduced by Article 14, paragraph 12, of Law no. 183 of 12 November 2011 ("*Provisions for the formation of the State's annual and multiyear budgets – 2012 Law of Stability*"), the Company decided to assign the duties of Supervisory Body to the Board of Statutory Auditors.
Official notification of said assignment to the Board of Statutory Auditors has been given to all company levels.

In performing said duties, the Board of Statutory Auditors operates keeping its activities carried out as the Supervisory Body from those performed in its capacity as the Company's auditors.

All provisions concerning the Supervisory Body contained in the Model, shall be deemed to refer to the Board of Statutory Auditors and to its exercise of those functions specifically assigned to it by the Decree.

3.2 Composition, duties and remuneration of the Supervisory Body

The Board of Statutory Auditors shall perform the functions of Supervisory Body for the entire period in which it remains in office and as composed pursuant to application of the rules governing the replacement, addition, suspension and cessation of office of its members, with

the exception of those cases, provided for in the following paragraphs, in which the composition of the Supervisory Body differs from that of the Board of Statutory Auditors.

The remuneration due for the Supervisory Body's performance of its duties shall be established by the Shareholders' Meeting at the time of the Board of Statutory Auditors' appointment.

As a rule, the Supervisory Body shall avail itself of the Company and Parent Company's structures to perform its supervisory and control tasks, first and foremost the Internal Auditing function, which is officially equipped with the technical know-how and the human and operating resources enabling it to guarantee the ongoing performance of checks, analyses and all other necessary requirements. The Internal Auditing function shall attend all of the Supervisory Body's meetings.
The Supervisory Body also makes use of Parent Company's structures appointed for such purposes, and of the corporate officers established in accordance with specific sector regulations to monitor specialised regulatory aspects (Employer, Health and Safety Officer, Personnel Safety Officer, the appointed Doctor, Anti-money Laundering Department Manager, Manager responsible for suspect transaction reports, Manager responsible for preparing the company financial reports, Environmental Affairs Officer pursuant to Legislative Decree no. 152/2006, etc.)

Where necessary, based on the specific nature of the issues addressed, the Supervisory Body may also avail itself of the services of external consultants.

Either directly or through the various corporate structures appointed for the purpose, the Supervisory Body, shall have access to all the activities carried out by the Company and the outsourcers, and to the relevant documentation, at both the central offices and the local branches of the Bank and of the outsourcers.
In order to be able to carry out its duties in a completely independent manner, the Supervisory Body shall avail itself of independent spending powers to be exercised on the basis of an annual estimated budget approved by the Board of Directors upon proposal from the Supervisory Body itself.

3.3 Eligibility requirements; grounds for disqualification from office and suspension

3.3.1 Professionalism, integrity and independence requirements

Without prejudice to the integrity, professional and independence requirements provided for by the regulations in force, in order to assign the Board of Statutory Auditors additional powers so that it may better perform its duties as Supervisory Body, at least one of the standing members thereof must be chosen from among persons possessing specialist expertise resulting, for instance, from having performed for at least three years professional activities in fields relating to the Company's sector of activity and/or from having an appropriate knowledge of the Company's organisation, control systems and main processes, or from having been – or from being –a member of the Supervisory Body.

In addition to meeting the abovementioned requirements, standing members and alternate members must also meet the following, further **integrity requirements**, according to which members of the Supervisory Body may not be selected from among those persons who:

- have received a final sentence, even if the sentence has been conditionally suspended pursuant to Article 163 of the Criminal Code without prejudice to the effects of rehabilitation, for one of the criminal offences from among those to which Legislative Decree no. 231/01 applies, those referred to in Royal Decree no. 267/1942 (bankruptcy law) or for tax crimes. The term "sentence" also includes those sentences delivered under Article 444 of the Code of Criminal Procedure, without prejudice to the effects of the declaratory judgement of lapse of the offence under Article 445, paragraph 2, of the Italian Code of Criminal Procedure;
- have been members of the Supervisory Body in companies or entities which have received, even by means of final measures (including the ruling given pursuant to article 63 of Legislative Decree no. 231/01), those sanctions laid down in Article 9 of the same Decree, for unlawful acts committed during their term of office;
- have been subject to the application of accessory administrative penalties resulting in the temporary loss of the eligibility requirements or the temporary ban on the performance of administrative, management and control functions at intermediaries or companies with listed shares, pursuant to Legislative Decree no. 58/98 (Consolidated Law on Financial Intermediation, hereinafter also referred to as TUF) or Legislative Decree no. 385/93 (hereinafter also referred to as TUB).

3.3.2 Verification of requirements

The Supervisory Body shall verify, within 30 days from its appointment, whether: its standing members and its alternate members meet requirements based on a statement made by the individuals concerned, and shall notify the outcome of said verification procedure to the Board of Directors;

Any untruthful statement made for such purpose by a member of the Body, shall result in that person being disqualified from office.

3.3.3 Grounds for disqualification from office

After their appointment, the Supervisory Body's standing and alternate members **shall lapse from office**, if:

- they incur in revocation of, or disqualification from, their position as auditor, also as a consequence of losing the professionalism, integrity and independence requirements set out in the law or the Articles of Association);
- it is ascertained that they have been members of the Supervisory Body in companies or entities which have received, even by means of final measures (including the ruling given pursuant to article 63 of Legislative Decree no. 231/01), those sanctions laid down in Article 9 of the same Decree, for unlawful acts committed during their term of office;
- it is ascertained that they received a final sentence (where the term "sentence" also includes sentences delivered under Article 444 of the Code of Criminal Procedure), even where the sentence has been conditionally suspended pursuant to article 163 of the Criminal Code for one of the offences to which Legislative Decree no. 231/01 applies, for the offences referred to in Royal Decree no. 267/1942 or for tax crimes;
- are subject to the final application of accessory administrative penalties resulting in the temporary loss of the eligibility requirements or the temporary ban on the performance of administrative, management and control functions at intermediaries or companies with listed shares, pursuant to Legislative Decree no. 58/98 or Legislative Decree no. 385/1993.

The members of the Supervisory Body shall inform the Chairman of the Board of Directors, under their full responsibility, the occurrence of one of the above-mentioned grounds for disqualification from office.

In these and all other cases in which the Chairman of the Board of Directors becomes directly aware of occurrence of one of the grounds for disqualification from office, he shall stop any provisions to be taken as required by law and by the Articles of Association, in regard of the position of auditor, and promptly convene the Board of Directors to ensure that, at the earliest possible meeting following the Chairman's becoming aware of said occurrence – the Board

declares the disqualification from the position of member of the Supervisory Body of the person in question. At the same time – and provided that disqualification is not dependent upon cessation of the office of auditor, as in such case the rules set down in the Civil Code concerning the completion of the body in question will apply – the Board of Directors shall see to replacing the disqualified person with the oldest alternate auditor.

Where the disqualification from office concerns an alternate member, in the absence of provisions made by the shareholders' meeting for the replacement of said person, and in any case until the making of such provisions, the Board of Directors shall see to replacing the disqualified member.

3.3.4 Grounds for suspension

Members of the Supervisory Body are subject not only to the same **suspension conditions** as those which, under the applicable regulations, lead to lapse from the office of auditor, but also to the further conditions set out below:

- the Supervisory Body members are found to have been members of the Supervisory Body in companies or entities which have received, by non-final measure (including the ruling issued pursuant to Article 63 of the Legislative Decree no. 231/01), the sanctions laid down in Article 9 of the same Decree, concerning unlawful acts committed during their term of office;
- a non-final sentence, also suspended conditionally pursuant to Article 163 of the Criminal Code (where the term "sentence" also includes sentences delivered under Article 444 of the Code of Criminal Procedure) for one of the crimes to which Legislative Decree no. 231/01 applies or for the crimes referred to in Royal Decree no. 267/1942, or for tax crimes;
- indictment for one of the offences mentioned in the previous point;
- non-final application of accessory administrative penalties resulting in the temporary loss of the eligibility requirements or the temporary ban on the performance of administrative, management and control functions at intermediaries or companies with listed shares, pursuant to Legislative Decree no. 58/98 or Legislative Decree no. 385/1993.

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

In any case, the Chairman of the Board of Directors, if he becomes aware of occurrence of one of the above-mentioned grounds for suspension, without prejudice to any other measures to be

taken pursuant to the law and to the Articles of Association relating to the office of auditor – shall immediately convene the Board of Directors in order that, at its next meeting, it suspends the person that incurred one of the above-mentioned grounds from the office of Supervisory Body member. In such event, the oldest alternate auditor shall temporarily take the suspended member's place.

Save for different provisions of the law and regulations, the suspension shall not last beyond six months. After this limit has expired, the Chairman of the Board of Directors shall enter the possible revocation among the items to be addressed in the next Board meeting. Members not revoked shall be fully reinstated in office.

Should suspension concern the Chairman of the Supervisory Body, the chairmanship of said Body shall be taken over, for the entire duration thereof, by the longest-serving member, or in the case of two or more members having served for an equal length of time, by the oldest member.

3.4 Temporary inability of a standing member

Where a standing member of the Supervisory Body is temporarily unable to perform his duties or perform them with the necessary independence and freedom of judgment, such member must declare the reasons for such inability, and, where it is due to a potential conflict of interests, he/she shall declare the reason for such conflict and refrain from participating in the meetings of the Body or in the specific resolution which the conflict relates to, until such time as the inability ceases or is removed.

An illness or injury or other justified impediment that lasts more than three months and prevents participation in the meetings of the Body also constitutes a cause of temporary impediment.

In the event of the temporary inability of a member, that member's place shall be temporarily taken by the oldest alternate auditor; the alternate auditor in question shall cease to hold such office when the reason for his taking over ceases to exist.

Where the inability lasts more than six months, extendable to a further six months not more than twice, the Board of Directors may revoke the member thus incapacitated and replace him with another standing member.

3.5 Duties of the Supervisory Body

The Supervisory Body, in pursuit of its ordinary activity shall oversee in general:

- the efficiency, effectiveness and adequacy of the Model in preventing and fighting the offences covered by Legislative Decree no. 231/01, and of any offences which in the future might howsoever give rise to the company's administrative liability;
- compliance with the provisions of the Model by its addressees, assessing the consistency of actual behaviour with the Model and any discrepancy, through information flow analyses and the reports to be submitted by the heads of the various corporate functions;
- updating of the Model when and as necessary, making proposals to the competent corporate bodies, wherever amendments and/or additions become necessary as a consequence of significant breaches of the provisions of the Model, significant changes in the Company's organisational set-up and procedures, or of the adoption of new legislation in this area;
- the existence and effectiveness of the company's health and safety at work system;
- implementation of the personnel training activities (see Chapter 6.2 below);
- adequacy of procedures and channels for whistleblowing for the purposes of Legislative Decree no. 231/2001 or violations of the Model and their suitability to ensure the confidentiality of the identity of the whistleblower in the activities of management of reports;
- compliance with the prohibition of retaliatory or discriminatory acts, whether direct or indirect, against the whistleblower for reasons directly or indirectly related to the report;
- opening and performance of the disciplinary sanction procedure, following a verified breach of the Model;
- compliance with the principles and values of the Code of Ethics.

The Supervisory 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 the Legislative Decree 231/07.

In order to allow the Supervisory Body an overview of second-tier controls (compliance, anti-money laundering, administrative and financial governance) and third-tier 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 Supervisory Body assesses the adequacy of safeguards on the individual sensitive corporate activities and addresses any further action to strengthen the control plans proposed by the individual structures concerned.

The control activities based on specific protocols designed and regularly updated based on the results of the risk analysis and of the control actions.

Risk analysis is the ongoing process of prior identification, classification and assessment of the risks (external and internal) and of the internal controls, which is the basis for the 231 Audit Plan.

This plan, prepared annually, submitted for approval to the Supervisory Body, and subsequently presented to the Board of Directors, also takes into account any remarks and suggestions made in various respects by the corporate bodies.

During the control actions, the level of the controls present in the company's operations and processes is analysed in detail. Any weaknesses found are systematically reported to the Organisational units and to the other corporate functions concerned in order to make the rules, procedures and organisational structure more efficient and effective. Follow-up activity is also performed to verify that the planned actions are actually undertaken. The control functions report regularly to the Supervisory Body on the follow-up activity carried out.

The Supervisory Body can exchange information with the independent audit firm, if it deems it necessary or appropriate within the scope of their respective competences and responsibilities.

3.6 Procedures and frequency for reporting to the Corporate Bodies

Whenever it is deemed necessary or advisable, or where requested, the Supervisory Body shall report to the Board of Directors on operation of the Model and the fulfilment of the obligations laid down in the Decree.
The Supervisory Body shall, at least on a half-yearly basis, submit to the Board of Directors a specific report on the adequacy of and compliance with the Model, which shall cover:

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

Following examination by the Board of Directors, the Supervisory Body shall see to forwarding the report – complete with any observations formulated by the Board of Directors – to the Parent Company's Management Control Committee, through the Corporate Secretariat.

Chapter 4 - Information flows to the Supervisory Body

4.1 Information flows in the case of particular events or whistleblowing events

The Supervisory 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, professionals, self-employed or "para-subordinate" workers, commercial partners, etc.) about any events which may give rise to liability for Banca. pursuant to the Decree.

Detailed information based on precise and consistent factual elements must be reported without delay with regard to:

- the perpetration, or the reasonable conviction of the perpetration, of the offences within the scope of Legislative Decree no. 231/2001;
- breaches of the conduct or procedural rules laid down in this Model and in the regulations therein referred to.
- initiation of legal proceedings against managers/employees for offences provided for in Legislative Decree no. 231/01.

The reports may be also made anonymously:

- directly to the Supervisory Body by:
    - letter addressed to "Banca IMI S.p.A. – Organismo di Vigilanza, c/o Ufficio Segreteria Societaria, Largo Mattioli 3, 20121 Milan";

  or

    - e-mail to ODV231@bancaimi.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 Supervisory Body of any reports received and provides a statement of any related facts discovered.

The external parties, including those performing outsourced services on the Bank's behalf, may submit their reports directly to the Supervisory Body by one of the above-mentioned methods.

Moreover, pursuant to the various regulatory sources that provide for the adoption of internal whistleblowing systems concerning specific sectors (TUB, TUF, anti-money laundering

legislation, etc.), reports may be made by personnel[3], necessarily in non-anonymous form, in accordance with the provisions of the Group Policies on internal whistleblowing systems, as follows:

- through the Head of the Internal Auditing function as "Officer for internal reporting systems," to the address segnalazioni.violazioni@intesasanpaolo.com. In this way, those who have come to learn of them as a result of the functions performed may submit reports of the above information and, more generally, of facts or conduct that may constitute a violation of the rules governing banking and any other irregular conduct;
- via the Intesa Sanpaolo Management Control Committee at segnalazioniviolazioni.comitatoperilcontrollo@intesasanpaolo.com, as an alternative reserve channel, in the event that the Whistleblower considers that because of the nature of the report itself, the Internal Auditing function may potentially be in a conflict of interest situation. In this case, Intesa Sanpaolo's Management Control Committee will inform the Bank's Board of Statutory Auditors/Supervisory Body.

With reference to the aforementioned reports, the Head of the internal reporting systems or the Management Control Committee, as an alternative back-up channel, shall inform the Supervisory Body without delay of reports that make express reference to the predicate offences pursuant to Legislative Decree no. 231/2001 or violations of the Model.
If the outcome of the investigations carried out by the appointed function, as provided for in the "Group Policies on internal whistleblowing systems (whistleblowing)," reveals that predicate offences pursuant to Legislative Decree no. 231/2001 or violations of the Model have been committed, the communication to the Supervisory Body is carried out by that function.

The Supervisory Body shall assess the reports received and adopt the appropriate measures based on its reasonable assessment and under its discretion and responsibility; it may also hear the author of the report and/or the author of the alleged violation and shall provide reasons in writing for any refusal to start an internal enquiry.

The Supervisory Body shall take into consideration the report, including anonymous ones, which contain factual elements.

Banca IMI S.p.A. shall safeguard those making said reports, regardless of the channel used, from any type of retaliation, discrimination or penalisation and shall in any event maintain the

[3] For the purposes of Group Policies on internal whistleblowing systems, "personnel" means: “all employees and persons engaged on the basis of arrangements entailing their insertion in the organisational framework, even where the arrangements do not involve a regular employment contract.”

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, against the whistleblower for reasons directly or indirectly related to the report, are forbidden; Retaliatory dismissal and organisational measures having a direct or indirect negative effect on working conditions shall be null and void unless it is shown that they are not retaliatory in nature and are based on reasons unrelated to the report;
- the adoption of discriminatory measures may be reported to the National Labour Inspectorate;
- the disciplinary system provided for by the Decree, in implementation of which the sanctions indicated in Chapter 5 below are established, also applies to whoever:
  - violates confidentiality obligations on the identity of the whistleblower or prohibitions of discriminatory or retaliatory acts;
  - reports intentionally or with gross negligence facts that are groundless.

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

- via the Internal Auditing function or the legal function, information concerning measures and/or reports 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 no. 231/2001, if such investigations concern the Bank or its Employees or Corporate bodies or in any case involve the Bank's liability;

- via the Internal Auditing function, the information notice on facts, acts, events and omissions indicating the risk of infringement of the rules of the Decree detected by the corporate control functions as part of their activities and corrective actions;

- via Personnel the disciplinary proceedings initiated against employees.

Each corporate structure to which a specific role has been assigned in a phase of a sensitive process must promptly report to the Supervisory Body any actions it performs which depart significantly from those set out in the process description and the reason which have made such departure necessary or advisable.

In the case of events which might give rise to serious liability for Banca IMI S.p.A., the Internal Auditing function, acting in accordance with Legislative Decree no. 231/2001, shall promptly inform the Chairman of the Supervisory Body and shall prepare a specific report describing in detail the event, the risk, the personnel involved, the disciplinary measures adopted and the solutions put in place to avoid reoccurrence of the event.

4.2 Periodic information flows

The Supervisory 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 other Parent Company's competent structures and by the corporate officers established pursuant to specific sector regulations.

Information flows coming from the Organisational Units

Once a year, the heads of the Organisational Units involved in "sensitive processes" within the meaning of Legislative Decree No 231/2001 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 Supervisory 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 Supervisory Body for prior approval.

Information flows coming from the Compliance function

The reporting flows from the Compliance function to the Supervisory Body consists of:

- annual reports, describing the results of the activity carried out concerning the Model's adequacy and functioning, the changes made to processes and procedures (for this purpose making use of support from the Organisation and Process Governance and

Development functions) as well as 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 Supervisory Body a complete overview of the second and third-tier control actions taken by the structures responsible for the controls within each sensitive area.

Both documents are subject to a six-monthly update.

As required by the Group Anti-Bribery Guidelines, a copy of the "Compliance Report prepared in accordance with the Bank of Italy's supervisory regulations and the Joint Bank of Italy-Consob Regulation" is also sent to the Supervisory Body, which also provides disclosure on the monitoring of the risk of corruption.

Information flows coming from the Internal Audit function

The ordinary reporting flow from the Internal Auditing function to the Supervisory Body shall consist of six-monthly and annual reports, informing the Supervisory Body of the checks carried out and the control actions planned for the subsequent six months, in line with the annual Audit Plan. In the context of this report, summary evidence is provided of the reports, the details of which have highlighted sensitive issues for the purposes of Legislative Decree no. 231/01.

Where it deems it necessary, the Supervisory 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 coming from the Anti-Money laundering function

The periodic reporting flows of the Anti-Money Laundering function to the Supervisory Body consist of six-monthly and annual reports on the verifications carried out, on the initiatives undertaken, on the shortcomings detected and on the relative corrective actions to be taken, as well as on the staff training activity.

Information flows coming from the Employer pursuant to Legislative Decree no. 81/2008

The reporting flow from the Employer pursuant to Legislative Decree no. 81/2008 to the Supervisory 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 coming from the Principal pursuant to Legislative Decree no. 81/2008

The ordinary reporting flow from the Principal pursuant to articles 88 ff. of Legislative Decree no. 81/2008 to the Supervisory 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 of the Environmental Affairs Officer

The reporting flow from the Environmental Affairs Officer pursuant to Legislative Decree no. 152/06 to the Supervisory Body consists of annual reports on compliance with the provisions set out in environmental regulations, on the monitoring of changes in regulations and on the results of the activity carried out having regard to organisation and to the controls performed on the company's environmental management system.

Information flows coming from the Corporate Social Responsibility function

The reporting flow from the Corporate Social Responsibility function to the Supervisory Body consists of the annual report on compliance with the principles and values contained in the Intesa Sanpaolo Group Code of Ethics.

Information flows coming from the Personnel function

The reporting flow from the Personnel function consists of a report submitted at least once a year on the disciplinary measures taken against personnel during the reporting period, highlighting in particular events directly or indirectly connected to reports of illegal conduct provided for by the Decree or violations of the Model.

Information flows from the Organisation function

The reporting flow from the Organisation function (drawn up with the collaboration of the Organisation and Process Governance and Development functions) consists of an information note that is sent on a yearly basis about the main changes made to the organisational structure, their importance as per Legislative Decree 231/01, as well as the degree of alignment of the system of delegated powers.

Chapter 5 - The disciplinary system

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 criminal offences and administrative infringements covered by Legislative Decree no. 231/01 – by the disciplinary instruments established to control compliance with the required conduct.

Any conduct of the employees of Banca IMI 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 Anti-Bribery 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 all 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 Supervisory Body through the Internal Auditing function, 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 Personnel function.

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.

Any penalties against employees on secondment from other companies within the Group, shall be applied by the appointed Personnel function of the company to which such employees belong.

The type and entity of each of the sanctions established shall be defined, pursuant to the above-mentioned legislation, taking into account the degree of recklessness, lack of judgment, 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/administrative offences which said conduct may determine and which it is for the judicial authority to ascertain.
The Supervisory 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 Supervisory Body shall also receive a report at least once a year from the Personnel 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.

Professional and middle management personnel

1) **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 or of the directives and instructions issued by management or by one’s superiors” in the formulation already provided in point a) of the current Disciplinary Code;

2) **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 or of the directives and 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:
the adoption, during performance of activities pertaining to sensitive areas, of 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,

such conduct is equivalent to an “*infringement (.. .) constituting (. . .) a “severe” failure to fulfil one’s obligations*” in accordance with **point d)** of the current Disciplinary Code;

5) **dismissal with 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 continuation of employment*” in accordance with **point e)** of the current Disciplinary Code.

Executives

Where executives infringe the internal principles, rules and procedures set out in this Model or adopt, in performing activities pertaining to sensitive areas, 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 with 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 not 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.

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.

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.

Board of Directors members

Where the Model is infringed by members of the Board of Directors of Banca IMI S.p.A., the Board of Statutory Auditors shall adopt those measures it deems appropriate having regard to the nature of the infringement, in accordance with the current legislation.

Chapter 6 - Internal training and communication

The administrative liability regime laid out by the law and the Model adopted by the Bank form an overall system which must be reflected in the operational conduct of the Bank's Personnel.
To obtain appropriate Personnel response it is essential to implement a communication and training activity for the purpose of disseminating the contents of Legislative Decree no. 231/01 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 Supervisory Body, information flows to the Supervisory Body, the protections provided for whistleblowers, 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 personnel member's professional culture.
Based on this knowledge, the training and internal communications activities addressed to all personnel 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.

6.1 Internal communication

On being hired, new personnel members receive, together with the required recruitment documents, a copy of the Group's Model, Code of Ethics, Internal Code of Conduct and Anti-Bribery Guidelines. By signing a declaration, personnel 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 Bank's Model and associated rules (in particular the Group's Code of Ethics, the Group Internal Code of Conduct and the Group Anti-Bribery 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 personnel 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 (for example, 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 serving personnel members receive full, prompt information at all times.

6.2 Training

The training activities aim to make the Decree and the 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:

- target (the addressees of the actions and their position and role in the organisation);
- contents (subjects covered, relevant to the individuals’ roles);
- means of delivery (physical and remote teaching, collection of digital objects);
- 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:

- digital training for all staff;
- specific training initiatives 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 learning tools to be used via the “Training platform.”

The dashboard of the platform allows each participant to consult the basic training content on Decree 231/01, as well as any legislative updates, and verify their level of learning through a final test.

Specific training, where needed to supplement the fruition of the digital objects for all staff, aims to disseminate knowledge of the criminal/administrative offences, possible types of offence, and specific safeguards relating to different departments, and to refer to the proper application of the Model. The teaching method is strongly interactive and makes use of case studies.

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

All personnel targeted by the various training actions must participate in the training. Participation is monitored by the competent Personnel department, assisted by the various department/office heads, who will in particular be responsible to ensure that their subordinates actually use the distance learning 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 functions concerned.

The Supervisory Body shall monitor the progress of training activities also by means of the information forwarded by the Compliance function and may request periodic checks on the Personnel'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 the Legislative Decree no. 231/2001 provides that the Model shall "identify the activities within which offences may be committed".

Therefore, as described in paragraph 2.4, the types of predicate offences covered by the Decree have been analysed, and for each category the Bank's corporate areas at risk of such criminal/administrative offences have been identified.

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.

It shall be the Supervisory Body's task to continuously monitor the adequacy of this Model, in order to guarantee its constant functioning and compliance with the provisions of the Decree.

In view of the foregoing, when subsequent protocols make reference to the Bank's Structures and/or Functions, or more generally to the term "Structure", such shall be deemed also to refer to Structures and/or Functions of the Parent Company, and/or of other Companies within the Group when the activities in question are outsourced.

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 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;
- 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 and administrative offences relating to market abuse;
- Sensitive area concerning workplace health and safety offences;
- Sensitive area concerning computer crimes;

- Sensitive area concerning crimes against industry and trade and crimes involving breach of copyright.
- Sensitive area concerning offences against the environment.

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.

Law no. 190 of 6 November 2012 (the "anti-corruption law"), which entered into force on 28 November 2012, reformed the rules for the offences in question, making the punishments harsher, amending certain cases and adding new ones. Consequently, the offence of "*Illegal inducement to give or promise benefits*" was added to Art. 25 of the applicable Decree, whereas previously it was covered by the offence of "Extortion in office". It also introduced the corporate law offence of "*Corruption among individuals*", described in paragraph 7.4.

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, assume the involvement of a private individual and a public agent, i.e. a natural person who, for the purposes of criminal law, holds the position of "public official" and/or of "person in charge of a public service", as defined respectively in Articles 357 and 358 of the Criminal Code.

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"[4].

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 Italian Social Security Agency, authorised local health service doctors, tobacconists authorised to collect vehicle tax.

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

Purely by way of example, we may mention the following persons, who have been identified by case law as being Person in Charge of a Public Service: Payment collectors of the National Electricity Company (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 Person in Charge of a Public Service, 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.

The liability of employees and officers, as well as that of the Entity, can also arise if their conduct vis-à-vis public agents is that typical of private individuals as described for the above-mentioned offences.

It should be noted in particular that, under Article 322-bis of the Criminal Code, the conduct of the private individual – whether as bribe-giver or as the party induced to give or promise benefits −is a punishable criminal offence not only when involving Public Officials and Persons in Charge of a Public Service within the Italian Public Administration, but also when: i) persons holding corresponding functions or performing corresponding activities within European Community institutions, or within Entities established on the basis of the Treaties establishing the European Communities, or, lastly, within the other European Union Member States; ii) persons holding corresponding functions or performing corresponding activities within other third countries or international public organisations, provided that, in this case, the private individual pursues an

[4] 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 no. 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.

undue benefit for himself or others with reference to an international economic transaction or acts in order to obtain or maintain an economic or financial activity (for example, in order to avoid termination of a supply/works contract or the issue of a measure negatively affecting his economic activity).

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

Misappropriation of funds from the State (Article 316-bis Italian Penal Code)

This type of offence occurs when, after lawfully receiving loans, subsidies or grants from the Italian Government or the European Union for the implementation of works or activities in the public interest, a party does not use the funds so obtained for the purposes for which they were granted.

Misappropriation of funds from the state (Article 316-ter of the Italian Penal Code)

The offence is committed in the cases in which – by using or submitting false statements or documents, or by omitting due information – a party obtains grants, financing, subsidised loans or other similar contributions granted or issued by the State, by other Public Authorities or by the European Union without being entitled to them. This offence is committed regardless of the use to which the contributions are put, as the crime arises at the time when the contributions are obtained.

Fraud against the State or other public bodies (Article 640, paragraph 2, no. 1, 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 or any other Public Body.

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 to obtain public funds (Article 640-bis of the Italian Penal 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, no. 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 Italian Penal Code)

Computer fraud consists of altering the functioning of an IT or telecommunications system or of tampering with the data or software contained therein, obtaining unfair profit. This type of offence is relevant for the purposes of Legislative Decree no. 231/01 only where it is committed to the detriment of the State or other Public Bodies.

By way of example, such an offence 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 Person in Charge of a Public Service whoever, 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. Such force is applied with violence or threat of unfair damage (for example, the refusal to duly perform an action unless paid to do so), by means that do not leave the freedom of choice to the person under force, who is consequently considered the victim of the offence and exempt from punishment.

Therefore, the liability of Entities for "*Extortion*" arises, provided an interest or benefit to the Entity exists, 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 Person in Charge of a Public Service 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 Person in Charge of a Public Service.

Undue inducement to give or promise benefits (Article 319 quater of the Italian Penal Code)

This offence punishes the conduct of a person in charge of a public service or a public official who, abusing 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.

Therefore, corporate liability for "*illegal inducement to provide or promise benefit*" can arise, provided such is 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:

- inducements offered in concert with a public official or with a person in charge of a public service in relation to a third party;
- inducements offered 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 a public service agent;
- acceptance of inducements from a public official or a public service agent.

Bribery

The element common to all cases of bribery against the public administration consists in an agreement between a public official or a public service agent 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 of "*Illegal inducement to give or promise benefits*", which instead require 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 of "*Illegal inducement to give or promise benefits*"; the distinction is important, first and foremost, when determining the punishment to be inflicted upon the private individual, such punishment being softer in the case of "*Illegal inducement to give or promise benefits*".

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 following types of bribery are covered by Article 25 of Legislative Decree no. 231/01.

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

This type of offence occurs when a public official or a person in charge of a public service 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.

Consequently, there are extensive and widely diverse scenarios of subservience to the duty and of donations giving a generic appearance of preferential treatment[5].

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

This offence, also known as "direct bribery", consists in 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 person in charge of a public service who solicits such offer or promise without obtaining it.

7.2.2. Sensitive company activities

The sensitive activities identified by 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 contracts with the Public Administration;
- Management of the activities relating to the 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 funded training;
- Management of litigation and out-of-court settlements;

[5] 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 Person in Charge of a Public Service, which was required in order for the offence in question to apply, is no longer relevant.

- 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 personnel selection and recruitment process;

With reference to the sensitive activity concerning Management and use of the Group's computer systems and Information Assets, see protocol 7.8.2.1. We reproduce hereunder, for each of the above-mentioned sensitive activities, the protocols laying down the control principles and rules of conduct applicable to the 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 the Parent Company, by the other Group companies and/or third-party 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 Structures involved in the signing of any type of contracts with Public Administration bodies, concerning transactions such as, but not limited to:

- contracts for the underwritten or unsecured placement of financial instruments issued or held by the Public Administration;
- agreements for the provision of investment services (trading, execution of orders, receipt and transmission of orders, placement of financial instruments, investment advice) and bank contracts;
- financial, strategic and corporate advisory services;
- trading OTC derivatives also in the name, and on behalf, of other Companies within the Group.

Pursuant to Legislative Decree no. 231/01, the related contract signing process could in theory present opportunities for perpetration of the offences of "bribery"[6], in its various forms, of "*illegal inducement to give or promise benefits*" and of "*fraud to the detriment of the State or other public authority*."

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 for the conclusion of contractual relationships 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;

[6]As already stated, under Article 322-bis of the Criminal Code, the conduct of the bribe-giver and the 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 European Community institutions, or within Entities established on the basis of the Treaties establishing the European Communities, or, lastly, within the other European Union Member States; ii) persons holding corresponding functions or performing corresponding activities within other third countries or international public organisations, provided that, in this case, the bribe-giver or person accepting inducement pursues an undue benefit for himself or others with reference to an international economic transaction or acts in order to obtain or maintain an economic or financial activity (for example, in order to avoid the termination of a supply/works contract or the issue of a measure negatively affecting his economic activity).

- 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 authorising and/or negotiating powers with the public administration:
    - are identified and authorised within the framework of the Company's Regulations, Powers and delegated powers;
    - 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 in contracts with the Public Administration; the internal rules illustrate the above-mentioned authorisation mechanisms, indicating the corporate officials who hold the necessary powers.

- Separation of duties between the different 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 entrusted 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.

- Monitoring activities:
  - the documentation relating to conclusion of the contractual relationships shall be submitted for review 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, fiscal, reporting and other 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 information system and the paper trail:
  - each relevant stage of the agreements with the Public Administration must be recorded in specific written documents;
  - 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, including that pertaining to single transactions only, also 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.

- Reward and incentive systems: The reward and incentive systems must be able to ensure consistency with the provisions of the law, with the principles set out in this protocol, and with the provisions of the Code of Ethics, also by including appropriate corrective mechanisms to address any non-compliant conduct.

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, the Group Internal Code of Conduct and the Group Anti-Bribery Guidelines. More 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 duly identified and authorised;
- 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;
- personnel 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 to the Anti-Bribery Officer for assessment and for the completion of any formalities to the Supervisory Body in accordance with the provisions under paragraph 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 no. 231/2001 and of laws against bribery 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 remuneration to any employees or external consultants 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 employees or external consultants where it is not adequately justified 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 offence covered by Legislative Decree no. 231/01; more specifically, purely by way of example and without limitation it is forbidden to:

- present incomplete documents and/or communicate false or altered data and/or omit important information concerning the nature 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 (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. 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, payment of inducements in breach of the reference regulations and of company regulations, and more generally speaking, all banking or financial transactions which generate a loss for the Bank and a profit for the aforementioned persons (for example, the unjustified cancellation of a debt position and/or application of discounts or conditions not in line with market parameters);
- promise or 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 personnel 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 any external consultants without following substantiated and objective criteria addressing professionalism and expertise, competitiveness, price, integrity and the ability to provide effective, continuous 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, the Group Internal Code of Conduct and the Group Anti-Bribery Guidelines. This in order to prevent the risk of commission of bribery offences, in their various forms, and "*Illegal inducement to give or promise benefits*" offences which could arise from the possible choice of parties who are "close" to persons linked to the Public Administration and from the consequent possibility of facilitating the establishment/development of relationships aimed at award of the appointment.

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

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:

- the management of financial transactions with the Bank of Italy and/or the Ministry of the Economy and Finance;
- the management of placement contracts for underwritten or unsecured financial instruments issued or held by the Public Administration;
- the management of agreements for the provision of investment services (trading, execution of orders, receipt and transmission of orders, placement of financial instruments, investment advice) and bank contracts;
- the management of financial, strategic and corporate advisory services;
- of trading OTC derivatives also in the name, and on behalf, of other Companies within the Group;
- management of taxes acting in the role of withholding agent.

Pursuant to Legislative Decree no. 231/2001, the related processes could present opportunities for commission of the offences of "bribery"[7], in its various forms, of "*illegal inducement to give or promise benefits*" and of "*fraud to the detriment of the State or other public authority*."
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 financial transactions with the Bank of Italy and/or the Ministry of the Economy and Finance include the following activities:

[7]As already stated, under Article 322-bis of the Criminal Code, the conduct of the bribe-giver and the 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 European Community institutions, or within Entities established on the basis of the Treaties establishing the European Communities, or, lastly, within the other European Union Member States; ii) persons holding corresponding functions or performing corresponding activities within other third countries or international public organisations, provided that, in this case, the bribe-giver or person accepting inducement pursues an undue benefit for himself or others with reference to an international economic transaction or acts in order to obtain or maintain an economic or financial activity (for example, in order to avoid the termination of a supply/works contract or the issue of a measure negatively affecting his economic activity).

- 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 Ministry of the Economy and Finance (for example, repurchasing transactions, transfers, etc.).

The process of managing placement contracts for underwritten/unsecured financial instruments issued or held by the Public Administration, consists in the following phases:

- evaluation of the transaction’s feasibility (due diligence);
- approval of the transaction by the Bank’s Internal Committees where such is provided for by the respective regulations;
- marketing activities aimed at contacting potential investors;
- syndication activities (the formation of a consortium for the placement of underwritten or unsecured securities), the structuring of transactions with the issuer (price spread, bid price, date of signing, date of expiry, etc.), investigation of the security, etc.;
- stipulation of contracts with counterparties (issuing companies and the members of the consortium);
- placement with investors (distribution).

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

- consultancy (if necessary);
- receipt of order;
- fulfilment of order;
- confirmation to customer that order has been executed;
- quantification of due amount;
- clearing;
- settlement.

The process of managing contracts for the provision of financial, strategic and corporate advice, stipulated with Public Bodies, consists in the following phases:

- formulation of a working plan and the sharing of said plan with the Public Body (kick off);
- appointment of any necessary external advisors (lawyers, auditors, etc.);

- definition of deliverables by the various advisors;
- analysis of the feasibility of the transaction (definition of the valuation method, formulation of the valuation model, due diligence, etc.);
- structuring of the transaction;
- negotiations between the counterparties;
- signing of the contract by the counterparties;
- performance of the contract (signing) for merger, acquisition, divestment and restructuring transactions;
- settlement of the transaction (closing).

Management of the OTC derivative trading carried out also in the name of, and on behalf of, other entities within the Group, consists in the following phases:

- consultancy with the customer of Banca IMI or of the Parent Company/other company within the Group, or with the operator of the Parent Company/other company within the Group, regarding the contents of the contract, and the definition of said contents;
- receipt of order;
- fulfilment of order;
- confirmation to customer that order has been executed;
- quantification of due amount;
- clearing;
- 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;
- transferring the tax to the Tax Authority.

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 system set up to monitor the processes described above must be based on the following factors:

- 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 authorising and/or negotiating powers in the management of the contractual relations with the Public Administration:
    - are identified and authorised by specific Regulations describing in detail the Mission and the functions of each of the Bank's Structures;
    - 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;

- Separation 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.

- Reward and incentive systems: The reward and incentive systems must be able to ensure consistency with the provisions of the law, with the principles set out in this protocol, and with the provisions of the Code of Ethics, also by including appropriate corrective mechanisms to address any non-compliant conduct.

Principles 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, the Group Internal Code of Conduct and the Group Anti-Bribery Guidelines.

More 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;
- personnel 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 to the Anti-Bribery Officer for assessment and for the completion of any formalities to the Supervisory Body in accordance with the provisions under paragraph 4.1;
- if third parties are to be involved in the management/execution of 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 no. 231/2001 and of laws against bribery and undertake to comply with them;
- the payment of fees or remuneration to any employees or external consultants 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 employees or external consultants 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 No. 231/2001, and, more specifically by mere way of example, to:

- present incomplete documents and/or communicate false or altered data and/or omit important information concerning the nature 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 (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. 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, payment of incentives in breach of the reference regulations and of company regulations, and, more generally, all the 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, the Group Internal Code of Conduct and the Group Anti-Bribery Guidelines. This in order to prevent the risk of commission of bribery offences, in their

various forms, and “Illegal inducement to give or promise benefits” offences which could arise from the possible choice of parties who are “close” to persons linked to the Public Administration and to the consequent possibility of facilitating the establishment/development of relationships with the Bank.

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

7.2.2.3. Management of procedures for requesting authorisations from or fulfilling requirements for the public administration

Introduction

This protocol applies to all the Bank Structures involved in the management of the activities relating to the request for authorisation or fulfilment of requirements towards 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 the 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 Public Administration regarding requests for data and information (for example, bank inspections and requests regarding financial transactions, on the part of the Financial Police), assessments and inspections.
- Management of bank assessments.

Pursuant to Legislative Decree no. 231/2001, the above-mentioned activities could in theory present opportunities for the commission of the offences of bribery[8], in its various forms, "*Illegal inducement*" and "*Fraud to the detriment of the State or other public authority*."

It should be noted that the principles of control and conduct defined within the framework of this protocol conform to those adopted by the Parent Company and/or other companies within the Group, and as such they also apply to all the activities concentrated with the aforementioned outsourcers on the basis of the respective contracts

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 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.

[8]As already stated, under Article 322-bis of the Criminal Code, the conduct of the bribe-giver 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 European Community institutions, or within Entities established on the basis of the Treaties establishing the European Communities, or, lastly, within the other European Union Member States; ii) persons holding corresponding functions or performing corresponding activities within other third countries or international public organisations, provided that, in this case, the bribe-giver or person accepting inducement pursues an undue benefit for himself or others with reference to an international economic transaction or acts in order to obtain or maintain an economic or financial activity (for example, in order to avoid the termination of a supply/works contract or the issue of a measure negatively affecting his economic activity).

Control principles

The system set up to monitor the processes described above must be based on the following factors:

- Expressly defined authorisation levels. Specifically:
  - within each Structure, persons exercising authorising and/or negotiating powers in the management of the activities relating to requests for authorisations to the Public Administration:
    - are identified and authorised by specific Regulations describing in detail the Mission and the functions of each of the Bank's Structures;
    - only operate within the scope/portfolio of customers assigned to them by the head of the reference Structure;
  - relations with Public employees in the event of requests for data/information or 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.
  - the deeds that are binding upon the Bank must be signed by duly appointed persons only.

- Separation of duties between the various 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 stages 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 upon request (for example, bank inspections or requests for information regarding financial transactions by/from the Financial Police), are truthful, complete, congruent and supplied in a timely manner. the procedure may include, where advisable, specific controls in the presence of the parties concerned. 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 handed over to the Public Body for the request for authorisation or for performance of requirements or upon request (for example, bank

inspections or requests for information regarding financial transactions by/from the Financial Police), shall be kept on file by the competent Structure;

- the Head of the Structure in question, or another specifically designated personnel 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 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, the Group Internal Code of Conduct and the Group Anti-Bribery Guidelines.

More 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;
- personnel 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 to the Anti-Bribery Officer for assessment and for the completion of any formalities to the Supervisory Body in accordance with the provisions under paragraph 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 no. 231/2001 and laws on bribery and undertake to comply with them;
- the payment of fees or remuneration to any employees or external consultants 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 employees or external

consultants where it is not adequately justified by the type of work performed or to be performed.

- Within the context of the inspections carried out by Officials of the Public Administration at the Bank's offices, without prejudice to those situations in which said Officials request direct meetings with specifically chosen members of the Bank's personnel, at least two persons shall attend the meetings with the Officials themselves, if the inspection in question concerns the Structure to which they belong; otherwise, where the inspection is followed by Structures other than the one concerned by the verification (for example: Personnel, Organisation, Legal, Auditing and Compliance) only one person shall participate in 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 No. 231/2001, and, more specifically by mere way of example, to:

- delay without good reason the presentation of, or fail to communicate, the requested documents/data;
- Provide incomplete documentation and/or communicating false or modified data;
- Use deceit which could lead Public Entities in error;
- ask or induce members of the Public Administration to grant preferential treatment or omit due information in order to improperly influence the Public Administration's controls;
- 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. 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, the payment of inducements in breach of the reference regulations and of company regulations, and more generally, all the 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, continuous 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, the Group Internal Code of Conduct and the Anti-Bribery Guidelines. This in order to prevent the risk of commission of bribery offences, in their various forms, and "*Illegal inducement to give or promise benefits*" offences which could arise from the possible choice of parties who are "close" to persons linked to the Public Administration and to the consequent possibility of facilitating the establishment/development of relationships with the Bank.

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

7.2.2.4. Management of funded training

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);
- F.B.A. (Fondo Banche e Assicurazioni [Banks and Insurance Companies Fund]);
- Solidarity Fund for income and employment support and for the professional conversion and professional retraining of credit sector employees.

Pursuant to Legislative Decree no. 231/2001, the related process could in theory present opportunities for commission of the offences of "bribery"[9], in its various forms, "*Illegal inducement*", "*Aggravated fraud for the purpose of obtaining public funds*," "*Embezzlement against the state*" and "*Unlawful receipt of disbursements to the detriment of the state*."
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 stages:

- identification of initiatives eligible for financing;

[9]As already stated, under Article 322-bis of the Criminal Code, the conduct of the bribe-giver 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 European Community institutions, or within Entities established on the basis of the Treaties establishing the European Communities, or, lastly, within the other European Union Member States; ii) persons holding corresponding functions or performing corresponding activities within other third countries or international public organisations, provided that, in this case, the bribe-giver or person accepting inducement pursues an undue benefit for himself or others with reference to an international economic transaction or acts in order to obtain or maintain an economic or financial activity (for example, in order to avoid the termination of a supply/works contract or the issue of a measure negatively affecting his economic activity).

- 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 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 who, in the "management of funded training", exercise authorising and/or negotiating powers in relations with the funding Bodies:
    - are identified and authorised 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;
  - 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 personnel 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.

- Separation of duties between the persons involved, in order to ensure that maker and checker mechanism is in place in all stages 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 personnel 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.

- Traceability of the process both from an IT standpoint as well as with respect to documentation. 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, the Group Internal Code of Conduct and the Group Anti-Bribery Guidelines.

More 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 persons involved in the process and who are responsible for signing acts or documents which are relevant outside the Bank (e.g. application files, feasibility studies, project plans, etc.) must be specifically appointed;
- personnel 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 to the Anti-Bribery Officer for assessment and for the completion of any formalities to the Supervisory Body in accordance with the provisions under paragraph 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 no. 231/2001 and of laws on corruption and undertake to comply with them;
- the payment of fees or remuneration to any employees or external consultants 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 employees or external consultants 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 No. 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 (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. 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, payment of inducements in breach of the reference regulations and of company regulations, and in general all banking or financial transactions which generate a loss for the Bank and a profit for the public official (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, the Group Internal Code of Conduct and the Group Anti-Bribery Guidelines. This in order to prevent the risk of commission of bribery, in all its forms, and "illegal inducement to give or promise benefits" offences which could arise from the possible choice of parties who are "close" to persons linked to the Public Administration and to the consequent possibility of facilitating/fast tracking the application assessment process.

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

The 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.

7.2.2.5. 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 no. 231/2001, the related contract signing process could present opportunities for commission of the offences of "bribery"[10], in its various forms[11], "*Illegal inducement*" and "*Fraud to the detriment of the State or other public authority*" as well as of the offence of "*Inducing someone not to make declarations to the Judicial Authority or to make false declarations*."[12]

There is also the risk of commission of the offence of "*Bribery among private individuals*" and "*Incitement to private-to-private corruption*," described in paragraph 7.3.

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 stages, which are pursued under the responsibility of the Structures competent for litigation, in coordination with Banca IMI's Legal Affairs Structure and the Structure concerned by the dispute, and with any external professionals appointed:

[10]As already stated, under Article 322-bis of the Criminal Code, the conduct of the bribe-giver and the 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 European Community institutions, or within Entities established on the basis of the Treaties establishing the European Communities, or, lastly, within the other European Union Member States; ii) persons holding corresponding functions or performing corresponding activities within other third countries or international public organisations, provided that, in this case, the bribe-giver or person accepting inducement pursues an undue benefit for himself or others with reference to an international economic transaction or acts in order to obtain or maintain an economic or financial activity (for example, in order to avoid the termination of a supply/works contract or the issue of a measure negatively affecting his economic activity).

[11]Including "Bribery in judicial proceedings" (Article 319-ter, paragraph 1, of the Criminal Code).

[12]This offence, punished by Article 377-bis of the Criminal Code, is a predicate offence of the liability of entities pursuant to Article 25-novies of the Decree. Moreover, pursuant to Article 10 of Law no. 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 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.

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

- 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 procedures for management of the process are governed by the internal rules, which are developed and updated by the competent Structures of Banca IMI and/or of the Parent Company, 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: 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 is 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 set of rules illustrates these authorisation mechanisms, and indicates 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 personnel member.

- Separation 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 stage 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, the Group Internal Code of Conduct and the Group Anti-Bribery Guidelines.
More 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 no. 231/2001 and of laws on corruption and undertake to comply with them;
- the payment of the payment of fees or remuneration to any employees or external consultants 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 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;
- personnel 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 to the Anti-Bribery Officer for assessment and for the completion of any formalities to the Supervisory 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 offence covered by Legislative Decree no. 231/2001; 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 stages of the proceedings:
  - make any undue demand or exercise pressure upon judges or members of arbitration panels (including ancillary personnel 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 or 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 (beyond the accepted practice regarding courtesy gifts of limited value) and grant advantages or other benefits of any kind – directly or indirectly, on one's own behalf or for others –to senior representatives or to their subordinates, belonging to counterparty companies or companies related to the Bank, in order to unduly 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, payment of inducements in breach of the reference regulations or of company regulations, and more generally, all the 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 professionals shall refer to the criteria of clarity and availability of documentary evidence laid down in the Group's Code of Ethics, the Group Internal Code of Conduct and the Group Anti-Bribery Guidelines; this in order to prevent the risk of commission of bribery offences, in their various forms, and "*illegal inducement to give or promise benefits*" offences which could arise from the possible choice of parties who are "close" to persons linked to the public administration and to the consequent possibility of facilitating the establishment/development of relationships with the Bank.

The Structure Heads involved are obliged to fulfil all the requirements necessary to ensure the efficient and proper implementation of the control and conduct principles described in this protocol.

7.2.2.6. Management of relations with the Supervisory Authorities

Introduction

This protocol applies to all 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.

Pursuant to Legislative Decree no. 231/01, the related process could present opportunities for commission of the offences of "bribery"[13], in its various forms, "Illegal inducement" 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, which include:

- the European Central Bank;
- the Bank of Italy;
- Consob;
- the Data Protection Authority;
- the Italian Competition Authority (AGCM);
- the National Anti-Bribery Authority, for those cases where the bank operates as "public official" o "public service agent".

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

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;

[13]As already stated, under Article 322-bis of the Criminal Code, the conduct of the bribe-giver and the 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 European Community institutions, or within Entities established on the basis of the Treaties establishing the European Communities, or, lastly, within the other European Union Member States; ii) persons holding corresponding functions or performing corresponding activities within other third countries or international public organisations, provided that, in this case, the bribe-giver or person accepting inducement pursues an undue benefit for himself or others with reference to an international economic transaction or acts in order to obtain or maintain an economic or financial activity (for example, in order to avoid the termination of a supply/works contract or the issue of a measure negatively affecting his economic activity).

- providing replies and performing requirements in response to requests/demands of the Supervisory Authorities;
- handling relations with Officials of the Supervisory Authorities during inspections.
- handling relations with Officials of the Supervisory Authorities and with the Financial Police during personal hearings, searches and seizures carried out in accordance with Article 187-octies of the Consolidated Law on Finance.

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:
  - 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.

- Separation of duties between the persons involved in the process of managing relations with the Supervisory Authorities. Specifically:
  - with reference to the management of relations not relating to the ordinary operations of the Bank's structures, all correspondence sent to the Supervisory Authorities in respect of findings or remarks on corporate operations shall be checked by the Parent Company's competent Legal, Internal Auditing and Compliance functions before being sent;
  - the Head of the Structure concerned by the site inspection, after ascertaining the subject-matter of the inspection, shall designate the human resources responsible for handling relations with the Public Officials during their visit to the Bank. The competent Legal function, the Internal Auditing function, the Compliance function and, in especially important cases the Supervisory Body must be promptly informed of the inspection under way 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;
  - 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 the Legal, Internal Auditing, Compliance and Corporate Secretariat functions;
  - 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 personnel 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 personnel 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 Structures 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 Structures. 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, the Group Internal Code of Conduct and the Group Anti-Bribery Guidelines.

More 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;
- personnel members cannot accept any request for undue benefits or attempt 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 to the Anti-Bribery Officer for assessment and for the completion of any formalities to the Supervisory Body in accordance with the provisions under paragraph 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;
- when Officials attached to the Authorities carry out inspections at the Bank’s offices, except where the inspectors ask to speak directly with named Bank personnel members, the meetings with the inspectors shall be held by at least two persons, if they belong to the Structure concerned by the inspection; otherwise, where the inspection is followed by Structures other than the one concerned by the verification (for example: Personnel, Organisation, Legal, Auditing and Compliance) only one person shall participate in 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 No. 231/2001, and, more specifically by mere way of example, to:

- delay the production of, without due reason, or fail to produce, the requested documents/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 (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. 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, the payment of inducements in breach of the reference regulations and of company regulations, and more generally, all the 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 Structure Heads involved are obliged to fulfil all the requirements necessary to ensure the efficient and proper implementation of the control and conduct principles described in this protocol.

7.2.2.7. 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[14], 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.

Pursuant to Legislative Decree no. 231/2001, the related process could represent a possible instrument for the commission of "bribery"[15] in its various forms and "illegal inducement".

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, or by facilitating persons close to public officials, promising the assignment of posts or supply contracts.

There is also the risk of commission of the offences of "*Bribery among private individuals*" and "*Incitement to private-to-private corruption*," described in paragraph 7.3.

The aim is also to prevent the risk of acquiring goods or services of unlawful provenance, in particular, to prevent involvement in other crimes which the counterparty's business may be exposed to (crimes against industry and trade; in crimes involving breach of copyright and in crimes of "*Employment of illegal aliens and illicit intermediation and exploitation of labour*,"[16] etc.).

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.

---

[14] 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 paripassu with literary works and enjoy the same protection (Article 1 of Law no. 633 of 22 April 1941).

[15] As already stated, under Article 322-bis of the Criminal Code, the conduct of the bribe-giver and the 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 European Community institutions, or within Entities established on the basis of the Treaties establishing the European Communities, or, lastly, within the other European Union Member States; ii) persons holding corresponding functions or performing corresponding activities within other third countries or international public organisations, provided that, in this case, the bribe-giver or person accepting inducement pursues an undue benefit for himself or others with reference to an international economic transaction or acts in order to obtain or maintain an economic or financial activity (for example, in order to avoid the termination of a supply/works contract or the issue of a measure negatively affecting his economic activity).

[16] See paragraphs 7.4 and 7.9.

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 system set up to monitor the processes described above must be based on the following factors:

- 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. Internal regulations define the said licensing mechanisms and provide information on the company members to whom such powers have been assigned;
  - 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, or needs/supplies of limited value. Such suppliers must ensure and, on demand, must be able to prove by submitting adequate documentation, also with reference to their appointed sub-contractors:
    - having regard to the use of trademarks or distinctive marks and to the sale of goods or services – that they comply with the industrial property rights and copyright legislation and, in any case, the lawful origin of the goods supplied;
    - having regard to the workers employed, in 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.

- Separation of duties between the 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, including the performance of adequate due diligence in accordance with the Anti-Bribery Guidelines prior to commencing the relationship, and 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 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, the Group Internal Code of Conduct and the Group Anti-Bribery Guidelines.

More 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 no. 231/2001 and of laws on corruption and undertakes to comply with them;
- the payment of fees or remuneration to any employees or external consultants 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 employees or external consultants where it is not adequately justified by the type of work performed or to be performed.
- payments are to be made only to a bank account in the name of the supplier/adviser with whom the relationship is in place;

- it is not permitted to make payments in cash, in a country other than the country where the counterparty is based, or to a person or entity other than the counterparty.

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 offence 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;
- promise of pay/offer undue sums of money, gifts or 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 personnel in companies that are counterparties or in relationships with the Bank, in order to unduly favour the interests of the Bank, or threatening them with unfair damage for the same reasons. 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, payment of inducements in breach of the reference regulations and of company regulations, and more generally, all the 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 Structure Heads involved are obliged to fulfil all the requirements necessary to ensure the efficient and proper implementation of the control and conduct principles described in this protocol.

7.2.2.8. 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.).

Pursuant to Legislative Decree no. 231/2001, the related process could represent a possible instrument for the commission of "bribery"[17], in its various forms, and "illegal inducement""

There is also the risk of commission of the offences of "*Bribery among private individuals*" and "*Incitement to private-to-private corruption*," described in paragraph 7.3.

This 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

[17]As already stated, under Article 322-bis of the Criminal Code, the conduct of the bribe-giver and the 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 European Community institutions, or within Entities established on the basis of the Treaties establishing the European Communities, or, lastly, within the other European Union Member States; ii) persons holding corresponding functions or performing corresponding activities within other third countries or international public organisations, provided that, in this case, the bribe-giver or person accepting inducement pursues an undue benefit for himself or others with reference to an international economic transaction or acts in order to obtain or maintain an economic or financial activity (for example, in order to avoid the termination of a supply/works contract or the issue of a measure negatively affecting his economic activity).

.

officers and/or their personnel 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.

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.

Acts of business and/or institutional courtesy of modest value mean gifts or other benefits (such as, for example, invitations to sports events, shows, entertainment, complimentary tickets, etc.) given by or to the same person or entity with a total value of no more than €150 in the one calendar year.

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 [18] activity;
- 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.

[18] 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..

Control principles

The system set up to monitor the processes described above must be based on the following factors:

- 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 benefits exceeding a value of €150 are admissible on an exceptional basis considering the profile of the donor or recipient and, at any rate, within reasonable limits, upon prior authorisation by a supervisor holding a position of at least Head of Department or of an equivalent company organisational unit. The value limits provided, on an annual basis, for gifts and other benefits do not apply to entertainment expenses for meals, refreshments, events, receptions, and hospitality events that are attended by Bank officers and personnel, providing the expenses are strictly connected with business and reasonable in relation to commonly accepted business and/or institutional courtesy practices;
  - different user profiles are defined for accessing IT procedures, matching specific authorisation levels based on assigned functions;

- Separation of duties: between the 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.

- Monitoring activities:
  - the internal set of rules define the limits beyond which the procedures for donations to charities and sponsorships must be preceded by due diligence, with particular reference to the Anti-Bribery Guidelines established by the Structure concerned. Specifically, it provides for:

        - analysis and verification of the type of organisation and of its statutory purpose;
        - 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 judgment, 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, the Group Internal Code of Conduct and the Group Anti-Bribery 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, for donations, such entities must be non-profit organisations;
- any initiatives falling under one of the categories eligible for "sponsorships" cannot at the same time benefit from charitable contributions;
- donations and sponsorship may only be made to a bank account held by the beneficiary. It is not permitted to make payments in cash, in a country other than the country where the beneficiary is based, or to a person or entity other than the beneficiary.

In any event, it is forbidden to initiate, cooperate/give rise to conduct that could be considered an offence in terms of Legislative Decree No. 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 or are engaged in practices involving the infringement of human rights, or contrary to vivisection and environment protection rules. Likewise, 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, which are to be approved by the Anti-Bribery 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-Bribery Guidelines;
- promise or pay/offer undue sums of money, gifts, services free of charge (outside the accepted practices of courtesy gifts of limited 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. Personnel 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 to the Anti-Bribery

Officer for assessment and for the completion of any formalities to the Supervisory 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 personnel 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 Structure Heads involved are obliged to fulfil all the requirements necessary to ensure the efficient and proper implementation of the control and conduct principles described in this protocol.

7.2.2.9. Management of the selection and recruitment process

Introduction

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

The process could constitute a possible instrument for the commission of bribery[19], in its various forms, and "illegal inducement," as well as "*Bribery among private individuals*" and "*Incitement to private-to-private corruption*," (described in chapter 7.3).

This because non-transparent management of the personnel 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 offices and/or their personnel 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 judgment or to ensure any benefit for the Bank.

There is also the risk of commission of the offence of "*Employing illegal aliens*".

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 personnel selection and hiring process comprises the following steps:

- Personnel 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.
- Formalisation of the hiring

[19]As already stated, under Article 322-bis of the Criminal Code, the conduct of the bribe-giver and the 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 European Community institutions, or within Entities established on the basis of the Treaties establishing the European Communities, or, lastly, within the other European Union Member States; ii) persons holding corresponding functions or performing corresponding activities within other third countries or international public organisations, provided that, in this case, the bribe-giver or person accepting inducement pursues an undue benefit for himself or others with reference to an international economic transaction or acts in order to obtain or maintain an economic or financial activity (for example, in order to avoid the termination of a supply/works contract or the issue of a measure negatively affecting his economic activity).

.

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 system set up to monitor the processes described above must be based on the following factors:

- Expressly defined authorisation levels:
  - the personnel selection and recruitment process is centrally managed by the competent Structure which receives formal requests for the hiring of new personnel 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 personnel 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.
  - hiring of candidates must be authorized by the appointed Structures of the Parent Company.

- Separation 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.

- Monitoring activities:
  - during the selection process, each candidate has to fill specific forms, to ensure that the candidates' details are collected in a uniform manner;
  - before a recruitment is made, adequate due diligence should be conducted, especially with regard to the provisions of the Anti-Bribery 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 personnel selection and hiring process.

Rules of conduct

The Bank's structures howsoever involved in management of the personnel 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 Group's Code of Ethics, the Group Internal Code of Conduct and the Group Anti-Bribery Guidelines.

More specifically:

- personnel 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 be 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 to the Anti-Bribery Officer for assessment and for the completion of any formalities to the Supervisory Body in accordance with the provisions under paragraph 4.1;
- personnel should be recruited from a shortlist of candidates, except in the case of qualified specialist personnel, protected employee categories, and persons selected for management positions;
- the comparative assessment of candidates should be conducted on the basis of criteria focused on competence, professionalism, and experience for the role for which the Company is recruiting.
- if the hiring process concerns:
    - disabled personnel, 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 personnel selection and hiring process, the contracts entered into with such persons shall contain a specific declaration that they know the provisions of Legislative Decree no. 231/2001 and of laws on corruption and undertake to comply with them;

- the payment of fees or remuneration to any employees or external consultants 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 employees or external consultants where it is not adequately justified 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 offence covered by Legislative Decree no. 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 judgment or to induce them to grant the Bank any advantages;
- promise to hire or accede to requests to hire senior officers of their personnel 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 Structure Heads involved are obliged to fulfil all the requirements necessary to ensure the efficient and proper implementation of the control and conduct principles described in this protocol.

7.3. Sensitive Area concerning Corporate Offences

7.3.1 Types of offence

Introduction

Article 25-ter of Legislative Decree no. 231/01 covers the majority of 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[20].

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 offence have been defined for the common purpose of ensuring transparency in accounting documents and in 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 member of the Intesa Sanpaolo banking group, 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 offence referred to in Article 25-ter of Legislative Decree no. 231/01 are listed below.

False corporate reporting (Article 2621 of the Civil Code)

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

These offences are committed by conducts that with respect to the profit and loss, balance sheet or cash flow situation of the company or the group, consist in the conscious:

[20]Article 25-ter was amended by:

- Law no. 190/12, adding reference to the new offence of "*Bribery among private individuals*", envisaged in Article 2635, paragraph 3, of the Civil Code, entered into force on 28 November 2012;
- Law no. 69/15, which for corporate offences eliminated any references to the conditions for the liability of Entities which are partly different from ordinary conditions and reformed the offences of "*False corporate reporting*", entered into force on 14 June 2015.

- presentation of untrue material facts in financial statements, reports and other corporate disclosures, addressed to the shareholders or the general public;
- omission of important material facts whose disclosure is required by law.

In any case, the conduct is prosecuted by law when it is aimed at securing an unfair gain for the perpetrators or others and likely to significantly mislead recipients. Furthermore, the breach also occurs where it refers to assets held or administered by the company on behalf of third parties.

Where the false information pertains to companies other than listed companies or companies treated in the same way[21]:

- presentation of false material facts only features as the offence in question if it is contained in the corporate disclosures required by law and such facts are important;
- mitigated punishments and the cause of the exclusion of penalty apply where the fact is of a particularly insignificant nature[22].

False reports or communications from the audit firm (Article 27 of Legislative Decree no. 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 Legislative Decree no. 39/10 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.

[21]The companies listed in a regulated market at national or European Union level are treated as their parent companies, as the companies issuing the financial instruments for which admission has been requested to trading in stated markets or that are traded on an Italian multilateral trading facility, as well as the companies carrying out public offerings or anyway managing them.

[22] Please see Article 2621-*bis* of the Civil Code laying down less harsh punishments in the event of minor facts, taking account of the nature and the size of the company and of the modes or effects of the conduct, or where the facts concern the small-sized companies that may not be subject to the bankruptcy proceedings. In addition, Article 2621-*ter* of the Civil Code refers to the enforceability of Article 131-*bis* of the Criminal Code, which excludes the imposition of a punishment where, given the modes of the conduct and the slight damage or risk, the offence is particularly insignificant in nature and no customary pattern has emerged in the behaviour.

The main offenders in this type of crime are the heads of the audit firm (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 supervisory 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[23].

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 in 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[24], 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.

---

[23]Article 25 ter of Legislative Decree 231/01 even now refers to Article 2624 of the Civil Code which originally envisaged this offence, despite regulatory developments in the meantime. Indeed:

- Law no. 262/05 introduced Article 174-bis of the Consolidated Law on Finance, 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;
- after reform of statutory auditing regulations, both Article 2624 of the Civil Code and Article 174-bis of the Consolidated Law on Finance 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 39/10.

This development gave rise to serious doubts about the permanent qualification of corporate liability for such conduct. By judgement no. 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 39/10 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 231/01. 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 39/10, but do not constitute an offence for which corporate liability is presumed.

[24]Article 2625 of the Civil Code also contemplated the offence of obstruction of control of directors in relation to independent auditors. After reform of the statutory audit regulations the offence was removed from Article 2625 of the Civil Code and reformulated in Article 29 of Legislative Decree 39/10, and later depenalised, Legislative Decree 8/16, as Article 25-ter of Legislative Decree 231/01 was not subsequently amended by also adding a reference to the aforementioned Article 29, it seems to confirm that the offence of obstructing control in relation to independent auditors is not 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 21 seems to apply.

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.

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 a conflict of interest (article 2629-bis of the Italian Civil Code)

This offence occurs where a director or a member of the management board (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 Directors, 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 the 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.

Bribery among private individuals (Article 2635, paragraphs 1 and 3, of the Civil Code)

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

The offence of "Bribery among private individuals" includes the conduct of executives, general managers, managers responsible for preparing accounting documents, auditors, liquidators and other persons with managerial functions within a company or another private entity, as well as persons subject to their management or supervision who, even through third parties, solicit or receive undue money or other benefits for themselves or for others, or accept the promise thereof, in order to perform or omit an act contrary to the obligations inherent in their office or the obligations of loyalty to the company or private entity to which they belong.

The bribe-giver is also punished, that is to say the person who, even through a third party, offers, promises or gives money or other benefits not due to these individuals.

Those who make an offer or promise that is not accepted, or the representatives of companies or private bodies who solicit the giving or promise, if the solicitation is not accepted, are liable for the crime of "*Incitement to private-to-private corruption*[25]."

Only the conduct of the bribe-giver (offer, giving, or promise, whether accepted or not), and not that of the corrupted (acceptance or solicitation), constitute a predicate offence of the administrative liability of entities, if committed in the interest of the company/body to which the bribe-giver belongs.[26]

[25] The offence of incitement subsists only if the offer or promise is made to or the solicitation is formulated by executives, general managers, managers in charge of preparing accounting documents, auditors, liquidators or persons who perform managerial functions in a company or entity. The same conduct committed by/directed to employees who do not perform managerial functions does not constitute instigation

[26] The reform of the offence of "*Bribery among private individuals*" and the introduction of the offence of "*Incitement to private-to-private corruption*" were provided for by Legislative Decree no. 38/2017 in force since 14 April 2017. The acts committed before that date constituted bribery between private individuals only if the conduct actually resulted in an act contrary to the duties and in damage to the company to which

Both offences are punishable by a court of law.

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

Anyone obtaining a majority in the shareholders' meeting by simulation or fraud, in order to achieve an unfair profit for the offender or for others is punished with imprisonment.

Market rigging (Article 2637 of the Civil Code)

This offence refers to the conduct of anyone who spreads 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 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.

The penalties for market abuse and the related administrative responsibility apply to conducts referring to issuers of listed instruments or for which admission to trading on a regulated market is sought.

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 no. 58/1998)

The new Article 173-bis of Legislative Decree no. 58 of 24 February 1998 (the Consolidated Law on Finance), 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.

---

the corrupted individuals belonged, and did not affect private entities other than companies. The inclusion of private bodies would appear to be all-encompassing and not limited to associations and foundations with legal personality.

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 is not an offence in which corporate liability is presumed[27].

7.3.2 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 Board of Statutory Auditors and with the independent auditors;
- Management of periodic reporting;
- Preparation of the prospectuses
- Purchase, management and sale of equity interests and other assets;
- Management of relations with Supervisory Authorities.

Below follow, for the first three 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 the activities, specifying that, with particular reference to the offence of bribery between private individuals, since this is a case with a potential cross-cutting impact on all the Bank's activities, reference is also made to the sensitive activities already covered by the following protocols in so far as they contain principles that have their preventive effect also in relation to the aforementioned offence:

- Management of disputes and out-of-court settlements (paragraph 7.2.2.5);
- Management of the procedures for the procurement of goods and services and for the appointment of professional consultants (paragraph 7.2.2.7);
- Management of gifts, entertainment expenses, donations to charities and sponsorships (paragraph 7.2.2.8);
- Management of the personnel selection and recruitment procedures (paragraph 7.2.2.9);

In relation to the sensitive activities indicated in the last point (“Management of relations with Supervisory Authorities”), reference should be made to the protocol in paragraph 7.2.2.6 which

[27] Article 25-*ter* of Legislative Decree no. 231/01 even now makes no reference to Article 2623 of the Civil Code, which originally envisaged this offence. Law no. 262/05 repealed the regulation and introduced the current offence of false statements in prospectuses pursuant to Article 173-*bis* of Legislative Decree no. 58/98. As Article 25-*ter* of Legislative Decree no. 231/01 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 principle indicated in the Court of Cassation judgement referred to in Note 21 seems to apply.

specifically aims to prevent not only the offences of bribery, in its various forms, 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 the Parent Company, by the other Group companies and/or third-party outsourcers, on the basis of special service agreements.

7.3.2.1. Management of relations with the Board of Statutory Auditors and with 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 Board of Statutory Auditors and with the independent audit firm at the time of checks and audits performed to fulfil legal requirements.
Pursuant to Legislative Decree no. 231/01, 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 no. 39 of 27 January 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 7.3.1 above.
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 Board of Statutory Auditors and in the independent audit firm, 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 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 must be based on the following elements:

- Set authorisation levels. In particular, relations with the Board of Statutory Auditors and the independent audit firm shall be managed by the head of the reference structure or by the persons specifically appointed by him.

- Separation of duties is ensured between the persons involved in the process of managing relations with the Board of Statutory Auditors and the independent audit firm, in order to guarantee that a maker and checker mechanism is in place in all stages of the process.

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

- All requests for specific documents made by the Board of Statutory Auditors in pursuit of its monitoring and control duties, are promptly and fully met.

- All requests for specific documents made by the Independent audit firm 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 Audit Firm 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 Board of Statutory Auditors shall be systematically recorded and kept on file;
  - the supporting declarations for preparation of the Representation Letter, issued to the independent audit firm, shall be checked and filed, and shall be signed by the Executive in charge of preparing the corporate accounting documents and by the Chief Executive Officer;
  - 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 Board of Statutory Auditors and the independent audit firm.

Rules of conduct

The Banks Structures and Bodies howsoever involved in the management of relations with the Board of Statutory Auditors and the Independent Audit Firm, 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:

- the periodic reports to the Board of Statutory Auditors and the independent audit firm shall be submitted in a timely manner, and all requests and demands received from the same bodies shall be promptly replied to;
- the information concerning the relevant facts for monitoring purposes, pursuant to the Consolidated Law on Banking, the Consolidated Law on Finance, and Legislative Decree no. 231/2007, must be conveyed immediately;
- 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 Board of Statutory Auditors or by any of its members, or by the Independent Audit Firm 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 Board of Statutory Auditors and to the Auditors, within the sphere of their activity, including all documents submitted in electronic format;

In any case, it is forbidden to engage/collaborate in or induce conduct which may be identified in 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:

- delay without good reason the presentation of, or fail to communicate, the requested documents/data;
- present incomplete documents and data and/or communicate false or altered data;

- adopt deceitful conduct which might lead the Board of Statutory Auditors and the independent audit firm into error in the technical-economic assessment of the documents submitted;
- promise or give sums of money or other benefits to members of the Board of Statutory Auditors or of the independent audit firm, with the purpose of promoting or furthering the Bank's interests.

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

7.3.2.2. Management of periodic reporting

Introduction

This protocol applies to all the Bank structures involved in the preparation of the documents that contain corporate communications concerning the Bank's profit and loss, balance sheet and financial situation.

Pursuant to Legislative Decree no. 231/01, the process of preparing such documents might present opportunities for commission of the offence of "*False corporate reporting*", as set out in Articles 2621 and 2622 of the Civil Code.

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 bribery, in its various forms, "*Illegal inducement to give or promise benefits*," "*Bribery among private individuals*," and "*Incitement to private-to-private corruption*" as well as "*money laundering*" and "*self-laundering*" offences.

The process of preparing the documents in question is governed by guidelines contained in the special regulations approved by the management body of the Parent Company, with the favourable opinion of the control body, in response to the indications of Article 154-bis of the Consolidated Law on Finance, 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*," implemented by the resolution passed by Banca IMI S.p.A.'s Board of Directors, set out the reference principles and the roles and responsibilities assigned to the Bank's structures in respect of the process covered by Protocol, of which it forms and integral part. The said 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 Consolidated Law on Finance, in order to guarantee their reliability, and in particular in order that the system of internal controls regarding the formation of the financial statements and of all other financial communications at Group level be duly monitored; therefore, the procedures set out in the regulation constitute the detailed operational rules of this protocol.

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

Within the sensitive processes relating to financial reporting, a particularly important role is played by the activities required for preparation of the annual financial statements, the consolidated financial statements and the quarterly and half-yearly statements, feeding of the reporting package for the purposes of the Group's consolidated financial statements, calculation of fiscal charges, and fulfilment of direct and indirect tax obligations. Such activities fall under the following corporate processes:

- Management of the accounts and of supervisory communications;
- Management of the individual companies' financial statements and of the reporting package for the Group's consolidated financial statements;
- Management of tax obligations;

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 documents containing corporate communications concerning the Bank's profit and loss, balance sheet and financial situation must be prepared in accordance with the specific corporate and Group 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 and for determining the value of individual accounting entries;
- 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 Bank's data required for the drafting of the consolidated financial statements and for the forwarding of such data to the Parent Company.

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 of the Administrative function reporting to the Appointed Manager, who also represents the interface with the Parent Company's Administrative and Financial Governance Service, with which it cooperates in preparing the company's financial reports, and by the Internal Auditing function in performance of its activity.

- Separation of functions
  - the process of preparing the documents containing corporate communications concerning the Banks' profit and loss account, balance sheet and financial situation involves several Structures, which operate in the different phases of the process in accordance with the principles set out in the "*Guidelines for administrative and financial governance*".

- Monitoring activities:
  - the activities of preparing the documents containing corporate communications concerning the Bank's profit and loss account, 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 corrective actions undertaken.

- Process traceability including both the electronic and the paper trail:
  - the decision-making process for preparing the documents containing corporate communications 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 profit and loss and asset situation of the Bank (annual financial statements, reports on operations, quarterly and half-yearly reports, etc.) and of the Group (reporting package for the consolidated financial statements) 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, the Bank's structures shall 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 targeting preparation of the financial statements and of the other corporate reports, in order to provide shareholders and third parties with a true and fair view of the Bank's profit and loss, balance sheet and financial situation.

In any case, it is forbidden to engage/collaborate in or induce conduct which may be classified as belonging to one of the types of offence covered by Legislative Decree no. 231/2001; more specifically, purely by way of example and without limitation it is forbidden 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 the Bank's profit and loss, balance sheet and financial situation;
- omit data and information imposed by the law on the Bank's profit and loss, balance sheet and financial situation.

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

7.3.2.3. Preparation of the prospectuses

Introduction

This protocol applies to all the Bank Structures involved in preparation of the Prospectuses[28] 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 Consolidated Law on Finance, 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 offence (paragraph 7.3.1), 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 pubic 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 for the contents of the prospectuses;
- statement by the Manager Responsible for preparing the company's financial reports, pursuant to Article154-bis of the Consolidated Law on Finance (for own issues only);
- forwarding of the prospectuses and management of relations with the competent Authorities.

[28] Pursuant to Legislative Decree no. 58 of 24/2/1998 as subsequently amended (inter alia by Law no. 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.

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 is based on the following elements:

- Expressly defined authorisation levels:
  - the Bank, taking into account the provisions of Article 154-bis, paragraph 3 of the Consolidated Law on Finance, 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 (for own issues only);
  - 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.

- Separation of duties:
  - the Prospectus preparation process sees the participation of several Bank Structures, professionally supported by external legal firms, 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 stage 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 no. 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 concerning the "*Management and disclosure of information 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 No. 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 Structure Heads involved are obliged to fulfil all the requirements necessary to ensure the efficient and proper implementation of the control and conduct principles described in this protocol.

7.3.2.4 Purchase, management and sale of equity interests and other assets

Introduction

This protocol applies to all structures involved in the purchase, management and sale of equity investments - whether direct or indirect, qualified or non-qualified - in the capital of other companies, including equity investments in Special Purpose Acquisition Companies (hereinafter SPAC) in which the Bank holds the role of Co-Sponsor, or in other forms of investment/disinvestment similar to the acquisition/disposal of equity investments (such as, for example, convertible bonds or equity financial instruments) or other assets (such as non-performing loans, business units, assets and legal relationships identified in) or other assets (identified groups of non-performing loans, business units, goods, and legal transactions).

Pursuant to Legislative Decree no. 231/2001, the related process could present opportunities for committing the offences of "*Bribery among private individuals*," "*Incitement to private-to-private corruption*," and "*Failure to disclose conflicts of interest*."

Process description

The process involves the following stages:

- assessment of the feasibility of a transaction and/or identification of investment and/or funding opportunities;
- management of pre-contractual dealings and performance of preliminary activities for the signing of the contract (verification of regulatory requirements, due diligence, etc.);
- completion of the contract;
- management of tasks connected with the acquisition, management, and disposal of equity investments (including the appointment of representatives at the investee) and other assets.

With specific reference to the activities carried out by the Bank in sponsoring a SPAC, the process is divided into:

- identification of new SPAC opportunities and new partners;
- constitution of the pre-Initial Public Offering (IPO) vehicle;
- IPO;
- scouting;
- business combination or liquidation.

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 is based on the following elements:

- Expressly defined authorisation levels. Specifically:
  - persons exercising authorising and/or negotiating powers at every stage of the process:
    - are identified and authorised based on the specific role assigned to them in the company organisational chart or by the head of the reference Structure by means of internal delegation, to be kept on file by the same Structure;
  - all acts and documents which involve a commitment on the part of the Bank must be signed solely by persons who hold the necessary powers;
  - the powers and delegation system sets out the managerial autonomy with regard to equity investments; the internal rules illustrate the above-mentioned authorisation mechanisms, indicating the corporate officials who hold the necessary powers.

  With specific reference to the activities carried out by the Bank in sponsoring a SPAC:
  - the establishment of SPAC and the business combination are subject to the go-ahead/approval of organisational structures/bodies/persons of both the Bank and the Parent Company, subject to authorisation by a special management committee ("SPAC Investment Committee") which expresses a binding opinion on the investment proposals;

- Separation of duties between the persons involved in the process to ensure that maker and checker mechanism is in place in the stages of the process.

  With specific reference to the activities carried out by the Bank in sponsoring a SPAC:
  - the process always provides for the involvement of different bodies/persons/organisational structures of the Parent Company and the Bank;

- during the IPO phase, Banca IMI cannot take on the role of NoMad and Specialist and must always avail itself of at least one Joint Global Coordinator, in addition to the Bank itself;
- scouting, i.e., the search for target operating companies potentially subject to business combinations with the SPAC sponsored by the Bank, must be carried out by third parties other than the Bank itself;
- the performance of due diligence activities carried out in relation to the business combination involves both third parties (co-sponsors of the initiative) and the Bank, which is responsible for carrying out an independent assessment of the opportunity;
- specific conduct and segregation of roles are set out for employees of the Intesa Sanpaolo banking group who are part of the SPAC bodies;
- in the management of the target operating company, during the scouting/business combination phase, no employee, director, statutory auditor or key executive of the Intesa Sanpaolo banking group may be present.

- Monitoring activities:
  - verification of the assessment carried out in accordance with the provisions of internal regulations through the possible performance of specific due diligence (e.g., economic/financial, accounting, legal, tax, etc.) on the target company and on the counterparty, with particular regard to the provisions of the Anti-Bribery Guidelines;
  - assessment that the resolution contains the criteria for evaluating the transaction price in accordance with market practices;
  - assessment of compliance with legislative and regulatory requirements (e.g., regarding anti-money laundering);
  - assessment of the keeping and updating of the register of equity investments in place;
  - assessment of the process of periodic evaluation of existing equity investments as part of the preparation of the company and consolidated financial statements.

  With specific reference to the activities carried out by the Bank in sponsoring a SPAC:
  - the SPAC establishment and placement phase:
    - diligence on the Co-Sponsor in accordance with the Anti-Bribery Guidelines;
    - controls on the total investment in institutional SPACs and the amount per investment;
    - constant monitoring of the correct application of the principles and rules governing the appointment of members of the SPAC's corporate bodies,

both before and after appointment to identify situations of conflict of interest that may have arisen;
        - checks on the roles and commission levels of Banca IMI within the placement consortium;
        - checks on the subscription book during the IPO phase and on the trading activities of special shares;
        - checks on the share of special and ordinary shares that Banca IMI may hold;
    - business combination phase:
        - checks on compliance with Banca IMI's ban on scouting target companies;
        - assessment of the requirements relating to any existing credit and/or equity investment relationships between the Intesa Sanpaolo banking group and the target company (together with the target group to which the target company belongs), both in this phase and after completion of the transaction;
        - due diligence activities in relation to the business combination both by third parties (co-sponsors of the initiative) and in terms of an independent assessment by the Bank;
        - checks on the target company in terms of certified financial statements and requirements on the members of the administrative and control bodies.

- Process traceability including both the electronic and the paper trail:
    - each relevant stage of the activity governed by this protocol must be recorded in specific written documents;
    - any agreement/convention/contract/other obligation functional to the purchase, management and sale of equity investments and other assets is formalised in a document, duly signed by persons holding appropriate powers according to the powers and delegation system in place;
    - in order to allow the reconstruction of the responsibilities and reasons underlying the preliminary assessment carried out for the acquisition of the equity investment and the choices made in the management and sale of equity investments and other assets, each Structure is responsible for the filing and retention of the relevant documents produced also electronically under this protocol.

    - With specific reference to the activities carried out by the Bank in sponsoring a SPAC:

- the discussions and decisions of the bodies of the Parent Company and of the Bank, involved in the evaluation and authorisation procedures, are recorded in specific documents, which are duly filed;
- the roles and responsibilities of the actors, whether internal or external, involved in the initiatives are defined and regulated (in addition to the general internal regulations) in specific documents and/or acts (e.g., investment agreement between the Bank and other Co-Sponsors of the initiative, letters of intent between the various actors involved in the activities functional and related to raising capital, deeds of merger between the SPAC and the target companies);
- the results of the due diligence relating to the business combination opportunity carried out autonomously by the Bank are traced and filed by the proposing organisational structure. A summary of this assessment is also provided in the file to be submitted to the Bank's decision-making bodies and for the Parent Company's approval;
- the Bank will report periodically on the transactions carried out, also in order to allow monitoring of the project by the Group Risk Committee.

- Reward and incentive systems: The reward and incentive systems must be able to ensure consistency with the provisions of the law, with the principles set out in this protocol, and with the provisions of the Code of Ethics, also by including appropriate corrective mechanisms to address any non-compliant conduct.

Rules of conduct

The Structures howsoever involved in the purchase, management and disposal of equity investments and other 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, the Group Internal Code of Conduct and the Group Anti-Bribery Guidelines. More specifically:

- persons who have authorising and/or negotiating powers in the pre-contractual, contractual and management phase of equity investment relationships are identified and authorised based on the specific role assigned to them in the company organisational chart or by the head of the reference Structure by means of internal delegation, to be kept on file by the same Structure;
- the documents relating to contracts for the purchase, management and disposal of equity investments and other assets must comply with the general and special

regulations in force for the sector in question, also through recourse to the advisory services of the competent company functions and/or external professionals;

- the personnel may not respond to any request for money or other benefits of which they may be the recipient or become aware made by top management, or by their subordinates, belonging to counterparty companies or in relation to the Bank, for the purpose of carrying out or failing to carry out an act contrary to the obligations inherent in their office or obligations of loyalty and must immediately report it to their Supervisor; in turn, they must immediately forward any report received to the Internal Auditing function and to the Anti-Bribery Officer for assessment and for the completion of any formalities to the Supervisory Body in accordance with the provisions under paragraph 4.1;
- if third parties are to be involved in the process for the conclusion and/or management the contractual relationships instrumental to the purchase, management and disposal of equity investments and other assets, the contracts entered into with such persons shall contain a specific declaration that they know the provisions of Legislative Decree no. 231/2001 and of laws against bribery and undertake to comply with them;
- the payment of fees or remuneration to any employees or external consultants 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 employees or external consultants where it is not adequately justified by the type of work performed or to be performed.
- personnel designated by the Bank as members of the administrative body of an investee company is required to inform the latter - in the manner and within the time limits provided for in Article 2391 of the Civil Code - of the interest held, on behalf of the Bank or on his/her own behalf or on behalf of third parties, in a given transaction of the company in question, refraining from carrying out the transaction if the latter is a managing director.

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

- communicate false or modified data;
- promise or pay/offer sums of undue money, gifts or free services (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 responsible for preparing the company's financial reports, statutory auditors and liquidators of companies, or persons subject to their management or supervision in order to obtain the performance or omission of an act contrary to the obligations inherent in their office or to the obligations of loyalty with the aim of promoting or favouring 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 provided for in company regulations, and more generally, all the 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, the Group Internal Code of Conduct and the Group Anti-Bribery Guidelines.

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

7.4 Sensitive area concerning crimes with the purpose of terrorism or subversion of the democratic order, organised crime, transnational crimes and crimes against the person

7.4.1 Types of offence

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 the Intesa Sanpaolo Group'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 belonging to or close to criminal organisations, services or financial resources which may be instrumental to the pursuit of illegal activities.

The types of crimes in question are summarised below.

* * *

<u>Section I</u> - 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, by 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[29].

[29]Article 270-sexies of the Criminal Code considers as having terrorist purposes those forms of conduct 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, judgment no. 39504/2008) the expression "subversion of

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 offence presenting a higher risk of occurrence are those of "**Financing of conduct for the purposes of terrorism**" (article 270-quinquies.1, of the Criminal Code), "**Removal of goods or money subject to seizure**" (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.

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 made by Article 24-quater, paragraph 4, of Legislative Decree no. 231/01 clearly tends to avoid possible gaps in that it is intended to promote international cooperation for the repression of fundraising and financing in any form, intended for acts of terrorism in general or relating to sectors and methods at greater risk, which are the subject of international treaties (air and sea transport, diplomatic representation, nuclear power, etc.).

* * *

Section II - Organised crime offences

Article 24-ter of the Decree, inserted by Law no. 94/2009, firstly sets out a group of offences relating to the various forms of criminal organisations, namely:

---

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.

- 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 no. 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 secure votes by the use of the mafia-type method in exchange for the disbursement or the promise of money or other utility.

Lastly, the other two types of criminal association (Article 416, paragraphs 6 and 7, of the Criminal Code and Article 74 of Italian Presidential Decree no. 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 abuse of 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. 5c.c.p. code of criminal procedure).

These are offences laid down by the special laws on the subject (in particular Law no. 110/1975 and Law no. 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.

* * *

Section III - Transnational offences

The liability of Entities for this category of offence is laid down in Law no. 146/2006, in order to enhance the effectiveness of the fight against transnational 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-quater of Presidential Decree no. 43/1973) or for trafficking in drugs of abuse (Article 74 of Presidential Decree no. 309/1990)

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 no. 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 no. 286/1998)[30]

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[31].

The punishment is increased where at least two of the five 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; sexual or labour exploitation; 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 no.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 investigation by the authorities or arrest. The offence occurs even if the person so assisted cannot

[30]Offences relating to illegal immigration, even if they lack the characteristics of transnationality, entail liability pursuant to Legislative Decree 231/2001, as from 19 November 2017, the date of entry into force of Article 25-duodecies, paragraph 1-bis, of the Decree, introduced by Law no. 161/2017

[31] 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.

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 individuals

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 crimes are listed: "**Enslaving or keeping persons enslaved" (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 pornographic material" (Article 600-quater of the Criminal Code), "Tourism initiatives aimed at exploiting child prostitution" (Article 600-quinquies of the Criminal Code), "Solicitation of children" (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 1 provides for the administrative liability of the Entity for the crime against the individual 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 making financial and economic resources available to organisations or persons that commit any of the above-mentioned offences.

The crimes of this section also include the crimes of:

- **Employment of illegal aliens** (Article 22, paragraph 12-bis, Legislative Decree no. 286 of 25 July 1998 – Consolidated Law on Immigration, referred to in Article 25-duodecies of the Decree[32]), 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, as for the crime of

[32] Article 25-duodecies was introduced to Legislative Decree no. 231/2001 by Article 2, Legislative Decree no. 109 of 16 July 2012, in force from 9 August 2012.

exploiting migrant workers illustrated in the section above, is only provided for in certain aggravated circumstances[33].

- **Illicit intermediation and exploitation of labour** (Article 603-bis of the Criminal Code, referred to in Article 25-quinquies of the Decree[34]), which punishes those who, taking advantage of the workers' state of necessity, intermediate, use, hire or employ labour in conditions of exploitation. Exploitation indices include situations such as the payment of wages not in compliance with collective agreements, the repeated violation of regulations on working hours and rest periods, and the violation of regulations on safety and hygiene in the workplace;
- **Racism and xenophobia** (Article 604-bis, paragraph 3, of the Criminal Code, referred to in Article 25-terdecies of the Decree) which punishes inducement, incitement or propaganda of discrimination or violence on racial, ethnic, national or religious grounds, based on the denial or minimization of the Shoah or other crimes of genocide, war or against humanity.

Though the risk of this offence being committed by the Bank appears to be remote, that should nevertheless be borne in mind in the context of management of the personnel selection and recruitment process and in the procedures for procurement of goods and services and for professional appointments.

7.4.2 Sensitive company activities

The risk of the commission of crimes with the purpose of terrorism or subversion of the democratic order, organised crime, transnational crimes and crimes against the individual mainly concerns, for banking operations, the establishment of relations with customers, the transfer of funds, “teller” transactions and, in particular, the credit granting process, an activity which, to ensure prevention of the offences in question, must be based on the fundamental principle of appropriate knowledge of the customers. This principle represents one of the key requirements established by Legislative Decree no. 231/2007 concerning prevention of the use of the financial system for the purpose of money laundering and of financing terrorism.

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

[33] 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.

[34] Reference to Article 603-bis was added to Article 25-quinquies of the Decree by article 6 of Law no. 199/2016, in force since 4/11/2016.

financial fight against terrorism and money laundering are considered to be appropriate also for the purpose of preventing the above-mentioned offences.

Furthermore, with regard to the offences of;

- "*inducement not to make or to make false statements to judicial authorities*", the company activity considered to be most sensitive in this respect is the management of disputes and their settlement;
- "*Employment of illegal aliens*," and the "*Illicit intermediation and exploitation of labour*" are company activities considered sensitive; as regards the former, the activity is that relating to management of the personnel selection and recruitment process and, as regards both, the activity to purchase goods, services and professional assignments.

Accordingly, for these offences reference is made to the protocols contained respectively in paragraph 7.5.2.1 "*Financial fight against terrorism and money laundering*," paragraph 7.2.2.5 "*Management of disputes and out-of-court settlements*," paragraph 7.2.2.9 "*Management of the personnel selection and recruitment process*" and paragraph 7.2.2.7 "*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 the Parent Company, by the other Group companies and/or third-party outsourcers, on the basis of special service agreements.

7.5 Sensitive area concerning receipt of stolen goods, money laundering and use of money, goods or benefits of unlawful origin, as well as self-laundering

7.5.1 Types of offence

Introduction

Legislative Decree no. 231 of 21 November2007, (hereinafter, the anti-Money Laundering Decree) and Legislative Decree no. 109 of 22 June2007, which transposed Community law have comprehensively consolidated 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 no. 231/2001, introduced by the anti-money laundering Decree, extended liability to cover the receipt of stolen goods, money laundering and unlawful use, also in the event that these acts are committed for terrorist purposes or for subversion of the democratic order as covered by paragraph 7.4 or they do not have the transnational characteristics provided for in the preceding provisions[35]. Lately, Article 25-octies has been amended by adding the new self-laundering offence[36].

The reinforcement of legislation on the administrative liability of Entities aims at preventing and combating 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 obligated parties (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 does not give rise to the Entity's administrative liability under Legislative Decree no. 231/2001, since such offences are not included in the list of the so-

[35] It should be noted that pursuant to paragraphs 5 and 6 of Article 10 of Law no. 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.

[36] The new self-laundering offence has been included in the Criminal Code and added to the predicate offences under Legislative Decree no. 231/2001 by Law no. 186/2014, which entered into force on 1 January 2015.

called predicate offences (i.e. the offences giving rise to the Entity's administrative liability). However, such infringement is punishable pursuant to the anti-money laundering Decree, according to a preventive safeguard policy, 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.

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 an intentional offence or carries out other transactions in respect of such money, goods or assets, so as to obstruct identification of their criminal origin.

The 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 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 unlawful proceeds 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)

A person may be liable for self-laundering if, having committed or contributed to committing any crime without fault from which money, assets, or other utilities have been derived, he/she carries out transactions for them to be used, replaced or transferred in economic, financial, entrepreneurial or speculative activities, in such manners as to significantly prevent identification of their criminal origin.

Punishment may be excluded for any conducts consisting in the allocation of unlawful proceeds for merely personal use or enjoyment. The aggravation of the punishment applies where the fact is committed in the performance of a professional, banking, and financial activity and mitigation in the case of offender’s active repentance.

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 crimes typically aimed at the creation of illegal capital, (e.g.: Extortion in office, bribery, embezzlement, fraud, bankruptcy crimes, arms or drug trafficking, usury, fraud against EU funds, etc.) and tax offences could also result in proceeds which are then laundered or self-laundered, not just in the event of fraud (e.g. use of invoices for non-existent

transactions generating a false VAT credit to be deducted), but also in the event that the economic utility resulting from the offence merely consists in tax saving for failure to disburse the money deriving from the illicit activity (e.g., omitted or untrue tax return, for amounts beyond the threshold of criminal relevance).

.

Conduct and subjective element.

A person may be liable for the receipt of stolen goods, money laundering or unlawful re-use, as the case may be, if he/she is a third party not involved in the crime generating the unlawful proceeds and receives them from the offender (or from others, and is aware, however, of their illicit origin), in order to perform on them the conducts underlying such crimes.

On the other hand, the person may be liable for his/her collaboration in the crime generating the unlawful proceeds and, as a consequence, also in the subsequent offence of self-laundering, if the relevant conduct is identified in any person that may have offered a causal contribution of any kind, whether moral or material, to committing the original offence, e.g. by determining or enhancing the offender's criminal intent with the promise, long before committing the offence, of helping in proceeds laundering/utilisation.

Unlike as provided for money-laundering or illicit utilisation offences, the offence of self-laundering requires for the conduct to be characterised by any such modes as may significantly conceal the true criminal origin of the goods; the interpretation of the most innovative aspects of the legislation – that is the requirement of the actual obstacle and the lack of imposition of the punishment for the self-laundering offender in the event of personal use (which apparently should always be excluded when the original offence or the reuse occur as part a business activity) – shall necessarily be referred to the case-law enforcement of the new offence.

As to the subject 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 far as financial intermediaries are concerned, the Bank of Italy and 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.

Correlation with the original crime of the illicit proceeds.

The offences in this Sensitive Area occur in the event that the relevant conducts are subsequent to the full commission of the crime giving rise to the illicit proceeds, even if such conducts take place after crime expiry (e.g. by virtue of the statute of limitation or due to offender's death), or even if the perpetrator may not be charged or punished, or one of the conditions for bringing the case is not met (e.g., due to lack in filing the charge, or in the request filed by the Italian Ministry of Justice, such request being necessary to prosecute ordinary crimes committed abroad, pursuant to Articles 9 and 10 of the Criminal Code)[37].

7.5.2 Sensitive company activities

The risk of the commission in a banking environment of money laundering offences in their wider sense (including, therefore, self-laundering), appears indeed more pronounced, being a typical risk of the banking and financial circuit, basically with reference to relationships with customers and as the assumption of customers' involvement/collaboration in criminal activities; in particular, it concerns:

- the establishment and management of ongoing relations with customers;
- the transfer of funds;
- trading of 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 role played by strictly complying with the provisions laid down in the anti-money laundering Decree for the purposes of preventing the offence in question also derives from the following considerations. Firstly, it should be noted that the Decree - for the purpose of identifying the type of conducts which may result in money-laundering, provides for an obligation to report any suspicious transactions. Article 1 defines "transaction" as the transmission or processing of means of payment" and Article 2 provides a very extensive list of conducts which can qualify as money laundering, including those conducts that, for criminal purposes, may supplement the commission of the self-laundering offence, or the commission of the other offences in question, and therefore, if such acts are committed by the entity's employees or managers, they might also give rise to the entity's administrative liability. Finally, the above-mentioned list also includes typical conducts relating to other offences, such as aiding and abetting an offender (Article 378 of the Criminal

[37] With respect to the irrelevance of the expiry of an offence that is the necessary condition for another offence please see Article 170, paragraph 1, of the Criminal Code; with respect to the irrelevance of the lack of a condition for the imposition of the punishment or for bringing the case please see Article 648, paragraph 3, of the Criminal Code, which is referred to also in Articles 648-bis, 648-ter,and 648-ter.1 of the Criminal Code.

Code) which, where it is of a transnational nature (on this point see paragraph 7.5) can constitute a predicate offence for the administrative liability of Entities.

The risk may exhibit different features and appear less relevant if the banking enterprise is seen as a “company”, with reference to those areas in which the bank, including irrespective of the involvement of the typical activities, carries out operations on its own capital, fulfils accounting and tax requirements. Here, a widespread presence of safeguards and procedures exists, which has already been set out in sector legislation and in the legislation concerning listed companies, in order to ensure compliance with transparency, correctness, objectivity, and 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. It should also be noted that the protocols regulating other sensitive activities – such as the Management of disputes and of out-of-court settlements, the Management of the procedures for the procurement of goods and services and for the appointment of professional consultants; the Management of gifts, entertainment expenses, donations to charities and sponsorships – 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 above.

More in general, all protocols within this Model, as long as they are aimed at preventing any crimes that may generate illicit proceeds, must be understood as in place also to the effect of countering money laundering offences in their wider sense. Reference is made specifically to Sensitive Areas protocols concerning corporate offences - in particular the protocol related to the Management of periodic reporting (paragraph 7.3.2.2) –the crimes and the administrative offences that may be ascribed to market abuse and computer crimes.

All aforesaid protocols are supplemented by the detailed corporate regulations governing such activities and also applies to the monitoring of any activities performed by the Parent Company, by other Group companies and/or third-party outsourcers, on the basis of special service agreements.

7.5.2.1. 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 current corporate provisions are also incorporated by reference, in particular the “Guidelines for combating money laundering and the financing of terrorism and for managing embargoes”, the “Rules on the subject of Anti-money laundering and Combating the Financing of Terrorism” and the “Rules for managing Embargoes”.

This protocol applies to all structures involved in the sensitive activities identified above and in the control of the risks linked to anti-money laundering legislation.

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

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[38]) and subjective aspects (persons subject to strengthened control requirements; persons established in Countries/areas having privileged tax or anti-money laundering regimes such as those identified by the FATF as being “non-cooperative”, 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 and MEF (Ministry of Economics and Finance), ABI-UIF lists, 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);

[38]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.

- 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;
- 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 concerning recording of ongoing relationships and of transactions ordered by the customers and storage of associated information;
- 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;

- Separation 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, Separation of duties shall be organised as follows:

- the operators of 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 shall, if the transaction is found to be suspicious, report it to the Representative in charge of reporting on suspicious transactions;
- such Representative 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 the correctness and completeness of customer identification details according to a risk-based approach, 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 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 appointed structure 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.

- 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 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 personnel 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, even where they are split into several different transactions:
  - 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 relationships and transactions in the financial transaction database (AUI) and on the filing of documentation.

The 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 no. 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 Structure Heads involved are obliged to fulfil all the requirements necessary to ensure the efficient and proper implementation of the control and conduct principles described in this protocol.

7.6 Sensitive area concerning crimes and administrative offences relating to market abuse

7.6.1 Types of offence

Introduction

The Consolidated Law on Finance provides for the offences of “Insider dealing" and "Market manipulation," regulated by articles 184 and 185 respectively.

Articles 187-bis and 187-ter of the Consolidated Law on Finance provide for the administrative offences of “Abuse and illicit disclosure of inside information" and "market manipulation," the conduct of which is substantially identical to that already punished by the two offences mentioned above.

The liability of the entity in the interest of which the two types of criminal conduct are committed is established by Legislative Decree no. 231/2001 (Article 25-sexies), while for the two types of administrative offences the liability of the entity derives from the said Consolidated Law on Finance (Article 187-quinquies) which refers to the same principles, conditions and exemptions of Legislative Decree no. 231/2001, with the difference that, for these administrative offences, the liability of the entity subsists in any case in which it fails to provide proof that the perpetrator acted in his/her interest or in the interest of a third party. It should also be noted that the crime of market abuse in the broadest sense also includes the crime of stock manipulation (classified as a corporate crime: see above paragraph 7.3.1) concerning non-listed financial instruments or financial instruments for which a request for listing on a regulated market has not been made.

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 the implementation of this principle and for the repression of its violations are established by European Union legislation, with Directive 2014/57/EU (so-called MAD 2) and Regulation (EU) No 596/2014 (so-called MAR); and by the Italian legal system with Legislative Decree no. 107/2018, in force since 29 September 2018, which also rewrote the aforementioned sanctions provisions of the Consolidated Law on Finance.

1) Except for what is specified with reference to each of the different offences, the conduct punished may concern[39]: financial instruments admitted to trading or in respect of which a

[39] Pursuant to Article 183 of the Consolidated Law on Finance, the discipline of market abuse does not apply to monetary and public debt management activities or those relating to climate policy, as well as to programmes for the repurchase of own shares and the stabilisation of the price of transferable securities, in compliance with the rules set out in Article 5 of the MAR.

request was filed for admission to trading on a regulated market in Italy or other countries of the European Union;

2) financial instruments admitted to trading or in respect of which a request was filed for admission to trading on a multilateral trading facility (MTF) in Italy or another EU Member State;
3) financial instruments traded on an Italian or other EU organised trading facility (OTF);
4) other financial instruments not covered by the preceding items, traded outside the aforementioned trading facilities (OTC), or the price of which depends on or affects the prices of instruments traded on the facilities referred to in the preceding items, including credit default swaps and contracts for differences;
5) spot commodity contracts as defined by the MAR;
6) benchmarks as defined by the MAR;
7) trading within the EU of allowances for greenhouse gas emissions or other related products traded on authorised auction platforms pursuant to Regulation (EU) No 1031/2010.

Under Article 182 of the Consolidated Law on Finance, the offences punishable according to 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 an Italian MTF, or financial instruments traded on an Italian OTF.

Pursuant to Article 16 of the MAR, market operators and investment firms that manage a trading facility, as well as anyone who prepares or professionally executes transactions, must adopt effective devices, systems and procedures[40] to prevent, identify and report, without delay to the competent authorities, suspicious orders and transactions that may constitute insider dealing or market manipulation or even just attempts. Violation of these obligations is sanctioned by Article 187-ter.1 of the Consolidated Law on Finance; the Bank might also in theory become involved in the offence committed by the customer having regard to the concrete manner and circumstances of the transaction.

The following is a description of the cases of offences.

Insider trading (Article 184 of the Consolidated Law on Finance)

The criminal offence punishes those who abuse inside information that has come into their possession: (i) in the capacity as member of the administrative, management or supervisory bodies of the issuer; (ii) because they have an interest in the issuer's capital; (iii) by reason of the exercise of a work or professional activity or of a function or office; (iv) as a consequence of the preparation or commission of an offence (e.g. "*breaking into a computer system and extracting inside information*").

[40] The reporting procedures are set out by Consob pursuant to Article 4-duodecies of the Consolidated Law on Finance, in accordance with the rules on internal systems for reporting violations by personnel (whistleblowing).

An offence is committed by one of the indicated persons who[41]:

(a) buys, sells or carries out other transactions[42] in financial instruments, directly or indirectly on its own account or on behalf of a third party, using that information (insider trading);

b) communicates such information outside the normal exercise of employment or profession, or outside a market survey in accordance with the provisions of Article 11 of the MAR (so-called tipping);

c) recommends or induces others, on the basis of this information, to carry out some of the operations described above (so-called tuyautage).

Inside information means any information of a precise nature, which has not been made public[43], relating, directly or indirectly, to one or more issuers of financial instruments or to one or more financial instruments, which, if it were made public, would be likely to have a significant effect on the prices of those financial instruments or on the price of related derivative financial instruments[44]."

Insider information may also include: i) commodity derivatives dealers; ii) related spot commodity contracts; iii) greenhouse gas emission allowances or other related products, iv) information submitted by a customer in connection with pending orders in financial instruments of the customer which, if made public, would be likely to have a significant effect on the prices of those instruments, related spot commodity contracts or related derivative financial instruments.

The conduct is less severely punished, with a fine, if the transactions do not concern the Italian or EU regulated markets, but the financial instruments referred to in paragraphs 2), 3) and 4), as well as the exchange of allowances referred to in item 7 of the Introduction.

Within the scope of the Bank's typical operations, there are various types of offence that could entail the Bank's liability in the event that the offence is committed in its exclusive or concurrent interest. The risk is conceivable, for example in relation to proprietary trading activities: i) where the person who arranges or executes the transaction misuses inside information about a particular issuer, which has been learnt by the Bank in the execution of a mandate relating to investment banking activities; ii) when an operator carries out, on behalf of the Bank, transactions in advance of customer transactions on the same instruments (so-called front running[45]), since for the

[41] Article 184 of the Consolidated Law on Finance does not punish a so-called secondary insider, i.e., the person who has obtained the inside information in circumstances other than those listed, for example who uses the information communicated to him/her, even without recommendations or induction, by a qualified person.

[42] It also includes operations to cancel or amend a previous order issued before having access to inside information.

[43] Article 17 of the MAR provides for the cases, timing and methods of the obligation to disclose inside information to the public by issuers of financial instruments or of participant in the emission allowance market.

[44] The definition of inside information is established by Article 180, paragraph 1, letter b-ter, of the Consolidated Law on Finance, by simple reference to Article 7, paragraphs 1 to 4, of the MAR. Please refer to this standard for a detailed reconstruction, in particular regarding the concepts of "precise character" and "significant effect."

[45] Operating approach whereby unlawful use is made of inside information concerning pending customer orders, for the benefit of the intermediary itself, or for the benefit of another customer and in the interest, or for the benefit, of the intermediary itself.

purposes of these rules, information on customer orders still to be executed is classified as inside information. A unique circumstance could also arise in cases where a representative or employee of the Bank is a member of the corporate bodies of other companies, and takes advantage, for the benefit of the Bank, of inside information acquired from the company to which he/she has been appointed.

Market manipulation (Article 185 of the Consolidated Law on Finance)

The criminal offence of "*Market manipulation*" occurs when any person disseminates false information or sets up sham transactions or employs other devices likely to produce a significant alteration in the price of the financial instruments[46].

Conduct consisting of orders to trade or other transactions which, though it may give the market misleading signals or artificially fix the price, is justified for legitimate reasons and has been conducted in accordance with a market practice accepted by the competent authority of the reference market, pursuant to Article 13 of the MAR, shall not be punishable.

The conduct is less severely punished, with a fine, if the transactions do not concern the Italian or EU regulated markets, but the financial instruments referred to in paragraphs 2), 3) and 4), as well as the exchange of allowances referred to in item 7 of the Introduction.

Conduct is punishable including if it concerns:

- spot commodity contracts which are not wholesale energy products, where such contracts are likely to cause a significant change in the price or value of the financial instruments listed under 1) to 4) of the Introduction, or such financial instruments, including derivative contracts or derivatives for the transfer of credit risk, where the events are likely to cause a significant change in the price or value of a spot commodity contract, where such price or value depends on the prices or values of such financial instruments;
- benchmarks, as defined in Article 3, paragraph 1, no. 29) of the MAR.

Within the scope of the Bank's typical operations, there are various types of offence that could entail the Bank's liability in the event that the offence is committed in its exclusive or concurrent interest. The risk is conceivable both in the form of disclosure manipulation (e.g., through the distorted use of marketing communications or other disclosures, including commercial and promotional information, concerning issuers of financial instruments and/or listed financial instruments), and in the various forms of operational manipulation in the context of the Bank's

[46] For a more detailed description of transactions and devices that may give the market false or misleading information or fix the market price at an abnormal level, see Article 12 and Annex I of the MAR, which contains a non-exhaustive list of indicators of manipulation consisting of the use of false or misleading information, the fixing of prices and the use of fictitious instruments or other types of deception or contrivance.

activities on financial markets in proprietary trading, trading on own account hedged back to back with customers, market making, etc.

Administrative penalties: Abuse and illicit disclosure of inside information and market manipulation (Article 187-bis and Article 187-ter Consolidated Law on Finance)

As mentioned in the Introduction, specific administrative sanctions are envisaged for conduct that essentially corresponds to that forming the subject of the criminal offences (Articles 184 and 185 of the Consolidated Law on Finance).

In fact, the administrative offences referred to in Article 187-bis and Article 187-ter of the Consolidated Law on Finance, instead of describing the prohibited conduct, simply refer to the prohibitions on the abuse and illicit disclosure of inside information and market manipulation, as set out in Articles 14 and 15 of the MAR[47]. The reference to the definitions of the cases contained in European legislation entails a general reference also to the other provisions of the MAR which define the notions of abuse, illegal disclosure and manipulation and which constitute a reference source also for the aforementioned criminal cases, even though they do not make full reference to them.

The types of administrative offence, the application of which is the responsibility of Consob, could therefore affect a wider range of conduct[48], to the extent that they are considered relevant elements and methods taken up through direct reference to Articles 14 and 15 of the MAR (and consequently to the rules of the MAR itself that constitute its prerequisite) and that they are not for criminal conduct, which has been described without express reference to the MAR, except for limited aspects.

Another factor which could lead to a more extensive and effective application of administrative sanctions than criminal sanctions is that, while for a criminal offence it is necessary to prove intent, for an administrative offence it is sufficient to be at fault.

This does not exclude the possibility that, for the same facts, the same person may be prosecuted and punished, combining proceedings and sanctions, both as a crime and as an administrative offence: in this case, Article 187-terdecies of the Consolidated Law on Finance provides that the Judicial Authority and Consob must take into account - when imposing the sanctions of their respective competence on the persons who have committed the facts and on the entities that are liable for the crimes and administrative offences of their employees and top management - the

[47] The liability of the company for the administrative offence committed by its employees or top management is also outlined in Article 187-quinquies of the Consolidated Law on Finance by referring to the violation of the prohibitions set out in Articles 14 and 15 of the MAR. The entity is liable to a fine of €20,000 to €15 million, or up to 15% of turnover, if this is more than €15 million. The sanction is increased up to ten times the product or profit derived from the offence, if these are of significant entity. This sanction includes the confiscation of the product or the profit of the administrative offence.

[48] For example, the conduct of a secondary insider is not punishable under Article 184 of the Consolidated Law on Finance, but is instead punishable under Article 187-bis, by virtue of the full reference to Article 14 of the MAR.

sanctions that have already been imposed in the proceedings (criminal or administrative) first concluded and that in any case the collection of the second monetary sanction paid can only take place for the difference in excess of the amount of the first monetary sanction paid.[49]

7.6.2 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 inside information and of external communications for the purposes of prevention of criminal and administrative offences in the area of market abuse;
- Management of orders and of market transactions to prevent administrative and criminal offences linked to market abuse (with particular regard to so-called 'operating' market manipulation).

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.
Such protocols also apply to the monitoring of any activities performed by the Parent Company, by the other Group companies and/or third-party outsourcers, on the basis of special service agreements.

[49] The company could therefore be held liable for both administrative and criminal offences against one of its employees for the same acts. The sanctions provided for by the entity for the administrative offences indicated in the previous note could therefore be combined with the sanction for criminal offences, provided for by Article 25-sexies of Legislative Decree no. 231/2001, i.e., a pecuniary penalty of up to €1,549,000, increased up to ten times the product or profit obtained, if of significant entity.

7.6.2.1. Management and disclosure of inside information and 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 with access to inside information, in the meaning provided by current legislation and regulations, or who handle the Bank's 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, other than the compulsory "price sensitive" communications (which come within the process of management and disclosure of inside information).

The correct management of the process of disclosure and handling of inside information helps prevent commission of the criminal offence of insider trading or of the corresponding administrative breach, set out respectively in Articles 184 and 187-bis of the Consolidated Law on Finance.

Sound management of this process of management of the Bank's external communications, together with the correct management of the circulation and processing of inside information, 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 Consolidated Law on Finance – with regard to "information manipulation", ensuring adequate control of the potential risk of "dissemination of false or misleading information, rumours or news".

As concerns the prevention of "operational manipulation", reference is made to the protocol on the "*Management of market transactions to prevent the criminal offences and administrative infringements 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 competent structures of the Bank and/or Parent

Company 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 Bank has implemented the Group regulations on the management of inside information (Group Regulations for the Management of Inside Information of Intesa Sanpaolo) which provide for the adoption of internal organisational measures aimed at the management and timely disclosure to the public of inside information that directly concerns it, in compliance with the provisions contained in Articles 17 and 18 of the MAR. In particular, the organisational, management and control measures for inside information are aimed at ensuring conditions of correctness, efficiency and timeliness in the bank's information transparency, as well as the methods of dealing with information that could have a significant effect on the prices of the financial instruments issued by the Bank and traded on the relevant markets or even on the prices of related derivative financial instruments.

Based on the Bank's current organisational structure, the activities pertaining to the management and disclosure of inside information are carried out by the Parent Company or with the operative support of the Parent Company's competent Structures, and in any case the Bank's structures shall continue to meet those obligations pertaining to the correct use of inside information, including the internal informational obligations for the purposes of the Register of persons with access to inside information (the so-called Insider List), and the obligations regarding the provision of correct, transparent information to customers, market counterparties and third parties in general.

In order to ensure that all personnel are duly made aware of such, the principles of monitoring and of conduct applied by the Parent Company and shared by the Bank, designed to guarantee compliance with the primary and secondary regulations in question, with the principles of confidential information processing and of secrecy in handling information that is not of public domain, and with the principles of monitoring and conduct to be complied with by those Bank structures that have contact with third parties, are set out below.

The provisions of this protocol are designed to ensure the Bank's compliance with the regulations in force and with the principles of transparency, correctness, objectivity and traceability in the performance of those activities in question, subject to reference to those internal procedures governing the Bank's processes in full that constitute an integral part of the Model.

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 the specific relevant information and inside information and operating procedures for managing said information are governed by the internal rules developed and updated by the Parent Company's 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, the Parent Company and the companies belonging to the Group, and the financial instruments issued;
- the customer companies and the financial instruments they issue (e.g. when providing corporate finance services to listed customer companies);
- commodity derivatives relating to the related spot commodity contract;
- emission allowances or related auctioned products;
- information transmitted by a customer and/or concerning customer orders awaiting execution which are of a precise nature has not been made public and which relates, directly or indirectly, to one or more issuers of financial instruments or one or more financial instruments and which, if made public, could have a significant effect on the prices of those financial instruments or on the prices of related derivative financial instruments (which is relevant to the case of front running).

The specific relevant information and inside information concerning the Bank, or another company within the Group if such is accessible to the Bank, are identified based on the criteria set out in the Group's reference regulations and, by way of example, may concern an internal decision of the Bank itself (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 from activities performed on financial markets on one's own or third persons' behalf.

Inside information regarding third-party issuers or the financial instruments issued by the latter, derives from the Bank's standard business concerning both investment services and activities, and primary market activities and ancillary services(in particular, corporate finance services such as advisory services, M&A and extraordinary transactions on issuer's capital or debt, etc.), when

provided to listed securities issuers, or issuers of securities for which admission to trading on a regulated market has been requested, or issuers of securities admitted to trading on an MTF or OTF, or for which a request for admission to trading on an MTF has been made.

In order to ensure the traceability of access to inside information, the Parent Company has set up, and manages, pursuant to Article 18 of the MAR, a Register of persons having access to inside information: In order to ensure the correct and prompt updating of such Register, each employee or representative of the Bank is bound to fully cooperate, on the basis of a specific internal procedure, in reporting any relevant situations for registration on the Insider List; for other inside or confidential information falling outside the scope of Article 18 of the MAR and of the relevant implementation rules, the Parent Company has created a supplementary system for recording sensitive situations within its internal regulations.

With regard to the disclosure obligations to the public, the process of disclosing to the market 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 (where listed, or in relation to the substantial impact on the Group's profit and loss performance and asset situation), has been largely concentrated in the hands of the Parent Company. The Group Regulation for the management of privileged information provides for a process that is divided into the following phases:

- identifying the 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 Consolidated Law on Finance, if the communications concern directly the economic and financial reporting information of the Parent Company, Intesa Sanpaolo S.p.A., and of the Group;
- disclosure of inside information to the public.

With regard to further obligations of correctness and transparency in the disclosure of news, data and information, even concerning third party issuers, the Parent Company 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.

With regard to any divulgation of false or misleading information through studies or recommendations, in view of the fact that the Bank distributes the products drawn up by the Parent

Company, the respective criteria adopted in order to prevent all forms of market abuse shall be governed by the respective process of the Parent Company, by the Bank's internal procedures as far as concerns any unlawful interference in the drafting of studies for public consultation, and by the regulations governing the distribution of such information, in order to prevent any form of informational asymmetry connected to the timing of said distribution.

Control principles

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

- a series of procedures involving various levels of control/preventive authorization on the part of the Parent Company regarding the disclosure of price-sensitive information (see below);
- creation, by the Parent Company, of the Register of persons having access to inside information pursuant to Article 18 of the MAR: the internal regulations of the Parent Company outline the process for feeding and managing the Monitoring Lists and Insider Lists of which the Register is composed (activities carried out directly by the Bank for information concerning the Bank and centralised at the Parent Company as regards information relating to third-party issuers), as well as the corporate functions responsible for such management from time to time. Such corporate functions, each acting within the scope of its competence, are required to fulfil disclosure obligations towards the persons entered in the Register and shall comply with any request for access to the Register made by the competent Authorities;
- in addition to activating the Monitoring Lists or the insider list in the Register of persons who have access to inside information, at least the following protection measures, listed by way of non-exhaustive example, are adopted for information that directly concerns the Bank:
  - when a Monitoring List is activated, the information owner structure (hereinafter SOP) assigns a conventional code to the list, which must be used in the subject and in the text of subsequent communications dealing with the subject as an encrypted identification mode;
  - no specific relevant information must be transmitted to the employees of the SOP if such transmission is not previously authorised by the SOP manager who intends to transmit the information;
  - the possibility of access to the specific relevant information and to the Inside Information must be limited to the persons who need to operate there and whose registration on the relative Monitoring List or Insider List is immediately ensured;

- in any case, it is necessary to provide for the registration in the Monitoring Lists of all persons who have free access to the specific relevant information without further prior specific authorisation;
- any structure employee who comes to learn of the specific relevant information or inside information accidentally during the course of his or her activities must immediately report it to the Head of the SOP involved who, on the basis of the available evidence, shall ensure his or her timely inclusion in the appropriate open list and verify the soundness of the control measures laid down within his or her structure;

- 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 logistic measures of separation (known as the “Chinese Wall” or Information Barriers), in compliance with the Parent Company’s provisions, between the organisational Structures which provide corporate finance services and activities to "Corporate” customers (which for Banca IMI corresponds to the Investment Banking & Structured Finance area and to the Global Markets Solutions & Financing area) and those providing services and investment activities or a number of additional services to investors or financial markets (“Market” services) which in the case of Banca IMI corresponds to the Global Markets Securities area and to the Finance & Investments Area, and also between such structures and those functions producing studies and research, kept separate from the Bank from a corporate point of view as a result of physical measures of separation. This physical separation is designed in order that:
  - the Structures belonging to the Market side are not aware of the inside information known to the Structures belonging to the Corporate side;
  - the Market Structures are not accountable to the Corporate Structures, and are not able to gain knowledge of the other side’s transactions or activities, thus ensuring that the two sides operate independently and without influencing each other:
  - the Corporate Structures do not condition either the Market Structures in the latter’s performance of their duties, or the Structures tasked with preparing studies and researches for the Parent Company (the same restriction also holds for the Market Structures);
- Watch List procedures are put in place by the Parent Company, to monitor “sensitive” situations that may give rise to the risk of conflicts of interest between the Bank and its key customers or the market in general or among customers (Watch List), or to manage and monitor the circulation of any exchanges of inside or confidential information also between mutually segregated Structures and impose any specific operational restrictions as necessary (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 Parent Company Structures, on the information concerning products distributed by the Parent Company and the corresponding advertising messages;
- the supervision of media relations, of promotional activities and of the management of the website, is carried out by a dedicated Bank structure that operates in conjunction with the Parent Company's Structures responsible for external communications and relations.

All such measures are defined and regulated in greater detail in the guidelines, policies and internal regulations in force from time to time which form an integral and substantial part of this protocol.

With specific reference to the process of disclosing inside information to the market, involving the Bank's Structures and those of the Parent Company, the respective procedure includes the following steps:

- in the case of "price-sensitive" events which are subject to the decision of the Parent Company's Board of Directors, all related communications to the market must be approved by the Chairman of the Board that has adopted the decision, or upon specific delegation from said Chairman;

- in all other cases of events which might give rise to disclosure obligations, the Parent Company's Managing Director and CEO, supported by the competent Investor Relations function, shall assess the "price sensitivity of the information to be disclosed. The text of the press release shall be approved by the Parent Company's Managing Director and CEO;
- if the communications concern directly the economic and financial reporting information of the Parent Company, Intesa Sanpaolo S.p.A., and of the Group, the Parent Company's Manager responsible for preparing a company's financial reports shall issue the attestation provided for by Article 154-bis of the Consolidated Law on Finance;
- the Chairman of the Parent Company's Management Board shall authorise release to the market of the communiqués approved by the Parent Company's Management Board. The Parent Company's Managing Director and CEO shall inform the Chairman of the Parent Company's Board of Directors of the communiqués submitted for his approval;
- if the price-sensitive information concerns events that occur within the scope of Banca IMI's activities, the Board of Directors and/or the Chief Executive Officer and/or General Management of the Bank shall be responsible for identifying and reporting any circumstances and events that might have a bearing on such information and shall promptly contact the Parent Company's Investor Relations and External Relations functions to ensure proper discharge of associated market disclosure requirements;
- the Parent Company's Investor Relations function shall prepare press releases relating to information which is price sensitive for the Group, i.e. which refers to events occurring within the sphere of operations of the Parent Company and/or of Banca IMI having a substantial impact on the Group's profit and loss and balance sheet performance, which shall be submitted – after authorisation by the competent corporate bodies and via the External Relations function – to the competent Supervisory Authorities, via the N.I.S., (Network Information system) and to the media;
- if the information is price-sensitive exclusively for Banca IMI, in its capacity as issuer of financial instruments as per Article 182 of the Consolidated Law on Finance, and such information has a substantial impact on the Bank's profit and loss and balance sheet performance, but not on overall Group performance, the related press releases shall be prepared by Banca IMI and submitted by such – after obtaining the written authorisation of the Parent Company's Investor Relations and External Relations functions - to the competent Supervisory Authorities and to the media; should the communications directly concern final economic and financial information, Banca IMI's appointed Manager shall endorse such as provided for by Article 154-bis of the Consolidated Law on Finance;

- the Parent Company's Investor Relations function, in consultation with Rating Agencies and Investor Coverage, is responsible for managing relations with financial analysts and institutional investors for the purposes of disclosure of significant information, ensuring its uniformity and consistency, also where such information is disclosed via the internet;
- relations with rating agencies concerning the disclosure of significant information shall be managed by a dedicated corporate function of the Parent Company.

Rules of conduct

The Bank's Structures, as well as each employee or collaborator, which are howsoever involved in management and disclosure of privileged information and in external communications, 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, as implemented by the Bank

Specifically, with regard to the handling and disclosure of inside information:

- no personnel member may carry out transactions on financial instruments of the Bank, the Parent Company, Group Companies or third-party Companies having business relations with the Bank, where the Bank's Structures that arrange for, or carry out, such transactions have access to inside information on the issuer or the security, and where said personnel member is aware of the privileged nature of such information or would have been aware of it by exercising ordinary due diligence, if the measures of separation (the Chinese Walls) designed for such purpose prove incapable of preventing the circulation of the information in question, or of specific restrictions have been imposed. This prohibition applies to any type of transaction in financial instruments (for example: shares, bonds, warrants, covered warrants, options, futures);
- no personnel 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;
- all the information and documents acquired in the course of discharging one's duties, whether they concern the Bank, the Parent Company or the other Companies within the Group, and their financial instruments, or whether they concern 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;

- specific and inside information may be disclosed within the Structures of the Bank and of the Parent Company only to those personnel members who need knowledge of it in order to perform their normal duties and in compliance with existing Separation 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 traded securities, etc.) and in any case when they are not required to comply with a documented obligation of legal, regulatory, statutory or contractual confidentiality and are required, in particular with regard to relations with trading counterparties, to promptly sign specific confidentiality agreements. In any case, selective communication to third parties of the Specific Relevant Information and Inside Information is permitted only in compliance with all the precautions and measures aimed at preventing improper internal and external circulation. The obligation to register such persons in the monitoring lists or in the relative insider list remains unaffected;
- it is forbidden to make third parties carry out operations related to 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. Accordingly, such information should not be discussed in open space offices hosting different organisational units, in lifts, corridors, break areas, staff canteens, and restaurants, or on trains, aeroplanes, and buses, at airports and, as a general rule, in venues 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 Consolidated Law on Finance; in any case, the bank personnel 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;

- 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, personnel 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 personnel;
  - 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. This circumstance also includes the cases of involuntary disclosure of inside information. Under corporate regulations involuntary disclosure shall be immediately notified to the competent function in order for the press release to be issued promptly as specified in the procedure applicable in the event of disclosure on the market of price-sensitive information;

- 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.

With reference to the external communications process:

- it is forbidden to disclose, either to other personnel 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 circulate 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; All documents containing valuations such as, for example, "fairness opinion", "public recommendation" and "formal valuation" must also be drawn up on the basis of objective elements (financial statements, market practices, financial templates, etc.).

The Structure Heads involved are obliged to fulfil all the requirements necessary to ensure the efficient and proper implementation of the control and conduct principles described in this protocol.

7.6.2.2. 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 orders and market transactions in financial instruments.

The process of managing orders and 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.

With regard to prevention of the criminal offence and administrative breaches of "information manipulation" – which may consist in the dissemination of false or misleading information, rumours or news – reference is made to the protocol on "Management and disclosure of information and of external communications for the purposes of preventing criminal and administrative offences in the area of market abuse", which sets out the control and conduct principles to be applied in the process of managing the inside information and external communications which the Bank's operational Structures might acquire in performance of their assigned duties, or to the Bank's communications to the market and, in general, to all external parties.

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 orders and 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 or 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 transactions, for the purposes of this protocol, concerns own account and trading on behalf of third parties of the financial instruments referred to in Article 182 of the Consolidated Law on Finance, carried out either directly by the Bank or through third parties (specifically, brokers) who are sent the orders to be fulfilled.

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 the Parent Company's 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 the Bank's own account hedged back to back with customers, an automatic procedure and order monitoring are in place which selects suspicious transactions which are subsequently analysed. 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.
With regard to the proprietary trading transactions carried out by Banca IMI an automatic procedure is in place to control transactions in order to prevent the criminal offences and administrative infringements relating to market abuse.

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 is based on the principal elements listed below:

- Authorisation levels established on the basis of the current power and delegation system, 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;
  - operating limits based on the position and/or level of the personnel concerned.
  - the structuring of operations related to the provision of investment services, ancillary services and of market transactions.

- Organisational separation (Chinese Wall) between the Structures that have direct relations with the market, including the structures that carry out trading activities (on the Bank's own account or on behalf of third parties, and sales activities, and the structures of the Parent Bank that participate in the production of studies and research on issuers or listed financial instruments with respect to the Structures that have inside information at their disposal;

- The involvement of different individuals from the same Organizational unit, or from different Organizational Units, in the structuring of operations related to the provision of investment services, ancillary services and market transactions.

- Control activity on orders and purchase and sale transactions executed 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.

- The existence of Committees within the Bank, that monitor risks at the structure level and in regard of third parties involved in transactions, and that authorize entry into new markets or the introduction of new products subject to the involvement, where provided for, of the Parent Company’s New Products Committee.

- 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.

- Traceability of the process both from an IT standpoint as well as with respect to documentation: in particular, financial instrument purchase and sale transactions are managed through dedicated software systems, where all details of the transactions executed are saved.

- The setting out of general principles of operations management, in the detailed internal rules, which specifically address 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 trading activities, on own account or on account of third parties, as defined above, 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 as implemented by the Bank.

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 fulfil 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 Consolidated Law on Finance 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 divulgation of false or misleading information by those persons who give the orders or undertake the transactions, or by other persons connected to such persons;
- undertake transactions or give orders to trade before or after producing or disseminating, also through other persons, research or investment recommendations which are erroneous or biased or demonstrably influenced by material interest.

The Structure Heads involved are obliged to fulfil all the requirements necessary to ensure the efficient and proper implementation of the control and conduct principles described in this protocol.

7.7 Sensitive area concerning workplace health and safety offences

7.7.1 Types of offence

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 the protection of health and safety in the workplace (Legislative Decree no. 81 of 9 April 2008), which has profoundly reorganized the many sources of previous legislation on the subject with Article 30, has set out the characteristics that the Model must have to prevent the crimes under examination.

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: Legislative Decree no. 626 of 19.9.1994 which contained general provisions on the protection of workers' health and safety; Presidential Decree no. 547 of 27.4.1955 on accident prevention; Presidential Decree no. 303 of 19.3.1956 on workplace hygiene; Legislative Decree no. 626 of 19.9.1994 which contained general provisions on

the protection of workers' health and safety; and Legislative Decree no. 494 of 14.8.1996 on construction site safety.

The specific prevention requirements set out in sectorial 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.

7.7.2 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 protocol also applies to the monitoring of any activities performed by the Parent Company, by the other Group companies and/or third-party outsourcers, on the basis of special service agreements.

7.7.2.1 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 no. 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 report, 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 Health and Safety Officer, 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 "Guidelines for a Health and Safety Management System at Work (SGSL)" are hereby incorporated as set forth by UNI – INAIL (Italian Workers' Compensation Authority) in September 2001. To this end, the Risk Evaluation 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 specific 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 – Organisational and management models – of Legislative Decree no. 81/08.

The "Company's Prevention and Protection Management System" outlined in the above-mentioned document has been prepared on the basis of a quality system, more specifically, following the guidelines contained in BS 8800 (Guide to Occupational Health and Safety Management Systems) and in OHSAS 18001 Occupational Health and Safety Assessment Series. Furthermore, the Bank has chosen to obtain quality certification of the processes managed by the Prevention and Protection function in accordance with the ISO 9001 standard. 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. 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 stages:

- 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 stages:

- 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 stages 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 acknowledgment 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 stages:

- 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 and 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 art. 26; such activities can be further delegated to other specifically appointed persons.

The operating procedures for managing the process and identifying the structures/roles in charge of the different stages 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, are granted the broadest organisational autonomy and are endowed with the broadest 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 all stages of the above-mentioned process must be identified and authorised by an express provision of the internal rules or by means of internal delegation, to be issued and kept on file by the Employer/Principal, or by the persons appointed by them.

- Separation of the duties between the different persons/corporate roles involved in the process of managing the risks 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 personnel 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, where appointed, 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[50] activities, 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, plant, individuals, 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 projects;
- The Workers' Safety Representatives, where appointed, 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;

[50] Including emergencies, first aid, supply/works contract management, regular safety meetings, consultations with the workers' safety representatives.

- all workplaces shall be visited and assessed by persons meeting the legal requirements and having appropriate technical qualifications. The Competent Doctor and the Health and Safety Officer shall visit the workplaces where workers are exposed to specific risks and shall carry out spot checks in the other workplaces;
- 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 (e.g. asbestos, radon, high risk of fires) and at the temporary or mobile construction sites (Project supervisors, Safety coordinators, Designers, Project managers, etc.);
- the competent Structures identified by the Employer/Principal shall 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; to 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.

- Process traceability including both the electronic and the paper trail:
  - the use of computer systems for managing the data and documentation required by the Consolidated Law shall be in compliance with Article 53 of said Law;
  - 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;
- 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 no. 231/2001 and undertake to comply with them;
- avoid appointments of external consultants that are not made on substantiated and objective grounds centred on 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 no. 276/2003 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 the provisions of the law, the internal rules and the instructions issued by the corporate 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 offence covered by Legislative Decree no. 231/2001.
The Structure Heads involved are obliged to fulfil all the requirements necessary to ensure the efficient and proper implementation of the control and conduct principles described in this protocol.

7.8 Sensitive area concerning computer crimes

7.8.1 Types of offence

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 n. 231/2001 Article 24-bis, which lists the series of computer crimes which might give rise to the administrative liability of Entities.

The aforementioned law has also modified the code of criminal procedure and the provisions on the protection of personal data, essentially to facilitate the investigation of computer data, and allow for certain periods of storage of data relating to computer traffic.

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:” 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:” 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 no. 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 databases 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)

Installation of devices aimed at 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- punishes any person who, other than in the cases allowed by law, installs equipment designed to wiretap, block or interrupt communications, regardless of whether such events do actually occur. 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 offense, 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, while 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 offense, 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 and distribution of computer or telecommunication systems’ access codes (Article 615-quater of the Criminal Code)

Distribution of computer equipment, devices or computer programs for the purpose of damaging or interrupting a computer or a telecommunication system’s operations (Article 615-quinquies of the Criminal Code)

Article 615-quater punishes any person who, in order to obtain personal profit or profit for others or to cause damage to others, illegally obtains, reproduces, distributes, communicates or delivers codes, keywords or other methods suitable to access a system protected by security measures, or provides information for such purposes.

Article 615-quinquies punishes any person who procures, produces, reproduces, imports, spreads, communicates, delivers or makes 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.

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, forgery of private agreements, 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[51].

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.

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[52]. The author of the offence can

[51] On this point it should be noted that under the Digital Administration Code (Article 1, point p) of Legislative Decree no. 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.

[52] Under Article 1 points e) and f) of Legislative Decree no. 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

clearly 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).

* * *

More in general it should be noted that many 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 no. 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 also Article 64-ter of the Criminal Code, which punishes computer crimes against the State or another Public Body, is a predicate offence of the administrative liability of Entities; on this point, see paragraph 7.2.1.

7.8.2 Sensitive company activities

The Bank’s activities exposed to the risk of computer crimes and of unlawful handling of electronic data held by the company are those of 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 European and national legislation on the protection of personal data, to prevent and control risks in the field of information technology (IT), to protect its information assets of 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.

---

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.

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.

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 protocol also applies to the monitoring of any activities performed by the Parent Company, by the other Group companies and/or third-party outsourcers, on the basis of special service agreements.

7.8.2.1. Management and use of the Group's computer 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 no. 231/2001, the related processes could in theory present opportunities for commission of the computer crimes referred to in Article 24-bis, and of the offence of "*Computer crimes against the State or another Public Body*," laid down in Article 640-ter of the Criminal Code and referred to in Article 24 of the Decree. Furthermore, access to the computer networks could also provide a means for committing offences against intellectual property rights[53].

It should be noted that the principles of control and conduct defined within the framework of this protocol conform to those adopted by the Parent Company and/or other companies within the Group, and as such they also apply to all the activities carried out by the aforementioned outsourcers on the basis of the respective contracts

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.

[53] For description of the relevant conduct see paragraph 7.10.

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.
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 computer security events and managing information security crises;
- design and implementation of computer security solutions.

The fraud prevention process involves the following stages:

- identification of the appropriate measures to upgrade prevention;
- monitoring of developments in computer crimes, also with regard to any 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 stages:

- 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 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 to be defined within each operating step of the processes 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;

- Separation 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 and of emergency and crisis situations;
    - 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 personnel 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 stages 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.

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.

- 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, corrective 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 personnel 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 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.

More 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;
- 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 no. 231/2001 and undertake to comply with them;
- the payment of fees or remuneration to any employees or external consultants 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 employees or external consultants where it is not adequately justified 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 offence covered by Legislative Decree no. 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;
- 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, key loggers, 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;
- enter or transmit data, information or software in order to destroy, damage, make partly or totally unusable or hinder the operation of computer or telecommunications systems of public interest;
- hold, procure, reproduce or disseminate access codes or other suitable means of access to a system protected by security measures without authorisation;
- 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;
  - holding any means aimed at removing or circumventing software protection devices;
  - 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 electronic information present in the protected works or appearing in their notices to the public on the copyrights applicable to them;
  - importing, distributing, installing, selling, modifying or using devices for unscrambling restricted access audiovisual transmissions, also where these are receivable free of charge.

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

7.9 Sensitive area concerning crimes against industry and trade and crimes involving breach of copyright

7.9.1 Types of offence

Introduction

Law no. 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 no. 231/2001, Articles 25-bis and 25-bis.1 refer to offences set out in the Criminal Code relating to industry and trade[54], while Article 25-novies—in order to strengthen the fight against intellectual property piracy [55]and counter the serious economic damage it causes to authors and to the related industry—refers to offences set out in the copyright law (Law no. 633/1941). The offences in question are described hereunder.

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[56]

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

[54] Subsequent to the amendment introduced by Law no. 99/2009, Article 25-bis of Legislative Decree no. 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.

[55] Pursuant to Article 1 of Law no. 633/1941, intellectual works protected by copyright are those belonging to literature (including scientific and educational literature), music, the figurative arts, architecture, theatre, and film, irrespective of their form of expression. Computer software and data banks which by their choice of arrangement of materials constitute an intellectual creation of their author are also ranked as literary works.

[56] 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.

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[57]. 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 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.

[57] The Intellectual Property Code (Legislative Decree no. 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*".

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" no. 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; 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[58] likely to mislead the buyer about the origin, provenance or quality of the work or product. The offence occurs where the

[58] Article 181-bis, paragraph 8, of Law no. 633/1941 states that for the purposes of criminal law the SIAE mark is considered a distinctive mark of an intellectual work.

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 to lead the consumers to confuse the products with similar products (but of different origin, provenance or quality) bearing a genuine mark. The provision aims at safeguarding 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. The provision includes cases such as the counterfeiting and use of non-registered trademarks, the use of containers 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[59] and, for the purpose of making a profit, introducing in Italy, holding for sale, offering for sale and offering directly to consumers or putting into circulation such products bearing counterfeit indications or designations.

[59] 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"*.

Making available protected intellectual works in telecommunications networks without authorisation (Article 171, paragraph 1, point a-bis, Law no. 633/1941)

Aggravated unauthorised use of protected intellectual works (Article 171, paragraph 3, Law no. 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[60].

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 no. 633/1941)

The first paragraph of the Article, which refers to computer software[61], 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.

[60] See, for instance, Article 65 of Law no. 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.

[61] Pursuant to Article 2 no. 8, of Law no. 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[62], 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[63] 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 no. 633/1941)

This provision lists a long series of unlawful conducts – where committed for non-personal use and for profit-making purposes – concerning: intellectual property intended for television, movies, sale or rental of 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

[62] Under Article 2, no. 9, of Law no. 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.

[63] The right of the establisher of the database are regulated by Articles 102-bis and 102-ter of Law no. 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.

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 trafficking in devices which enable unauthorised access to such services or products aimed at circumventing the technology safeguards preventing 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 no. 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[64].

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. no. 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.

7.9.2 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;

[64] Under Article 181-bis, paragraph 3 of Law no. 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.

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 7.5.2.1 on "Financial fight against terrorism and money laundering";
- paragraph 7.2.2.7 "Management of the procedures regulating provision of goods and services and professional appointments",
- paragraph 7.2.2.8 on "Management of gifts, entertainment expenses, donations to charities and sponsorships";
- paragraph 7.8.2.1 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.

Such protocols also apply to the monitoring of any activities performed by the Parent Company, by the other Group companies and/or third-party outsourcers, on the basis of special service agreements.

7.10 Sensitive area concerning offences against the environment

7.10.1 Type of offence

Introduction

Article 25-undecies of Legislative Decree No. 231/2001 identifies offences against the environment, for which, based on Community law provisions, entities are administratively liable[65]. These offences are described in the Italian Criminal Code, in Legislative Decree No. 152/2006 (Environment Protection Policy, hereinafter referred to as E.P.P.) and in various special laws, both classified as criminal offences, as well as contraventions[66]. These cases are the following.

Environmental pollution (Article 452-bis of the Criminal Code)

This regulation punishes those who improperly cause significant and measurable water, air, ground or underground damage or deterioration in an ecosystem or of the biodiversity.

Environmental disaster (Article 452-quater of the Criminal Code)

This regulation punishes those who improperly cause an environmental disaster, whereby the balance of an ecosystem is altered irreversibly, or whose removal is particularly expensive and extraordinary, or public safety is jeopardised, because of the seriousness of the event, by extension, or for the effects, or for the number or people injured or exposed to the danger.

Trafficking and abandoning highly radioactive material (Article 452-sexies of the Criminal Code)

Several abuses are punished (transfer, purchase, receipt, transportation, import, export, possession, abandonment, etc.) with respect to highly radioactive materials.

Illegal association with environmental aggravation (Article 452-octies of the Criminal Code)

[65] Article 25-*undecies* of Legislative Decree No. 231/2001 by Legislative Decree No. 121/2011, in force since 16 August 2011, in the text initially introduced by Legislative Decree no. 121/11, application of Directive 2008/99/EC and Directive 2009/123/EC, and later amended by Law no. 68/15, in force since 29 May 2015, which supplemented the Criminal Code with the new crimes against the environment

[66]The offences are those listed in the Criminal Code (except for Articles 727-bisand 733-bis) and by the E.P.P. in articles 258 sub-article 4, second sentence, 260 c. 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. Environmental crimes and environmental disaster, where committed on the basis of fault, may be punished pursuant to Article 452-quinquies of the Criminal Code and they are also predicate offences giving rise to the Entity's administrative liability.

Under this regulation a specific punishment aggravation is set out for the offences of illegal association with the purpose of committing any of the environmental crimes envisaged in the Criminal Code. In the event of an offence by a mafia-type association, the aggravation is given by the takeover in the management or the control of economic activities, of concessions, permits, contracts or of public services on environmental matters.

Offences involving protected wild animals or plants or protected habitats (articles 727-bis and 733-bis of the Italian 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, E.P.P.)

Article 137 E.P.P punishes breach of the rules regulating discharges 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 E.P.P.

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 authorised discharges of rapidly biodegradable quantities.

Breach of waste management regulations (article 256, sub-articles 1, 3, 5 and 6, 1st part, E.P.P.)

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.

Omission of remediation in the cases of ground, underground, surface waters or groundwater pollution (article 257, sub-articles 1 and 2, E.P.P.)

Except for the case where a serious offence no longer applies (e.g.as in the above-mentioned circumstance set forth in Article 452-bis of the Criminal Code) a punishment is imposed to anyone who, having caused said pollution by exceeding the risk threshold concentrations, does not inform the competent authorities and fails to proceed with site remediation in compliance with article 242 E.P.P. Successful remediation is a condition for the exclusion of punishment including for the environmental contraventions laid down in other special laws for the same event.

False certification of waste analysis (article 258, sub-article 4,-2° part, E.P.P.)

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, E.P.P)

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, paragraphs 1 and 2, of the Criminal Code)[67]

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, E.P.P.)

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

[67] Legislative Decree no. 21/2018 (Official Gazette no. 68 of 22/03/2018) sets out the crime of "Activities organized for the illicit trafficking of waste" in Article 452 quaterdecies, paragraphs 1 and 2, of the Criminal Code.

volunteer to participate in the IT system of control on the origin of waste known as SISTRI. In this respect, offences consisting in providing false information on the nature and characteristics of waste in order to obtain a waste analysis certificate 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, E.P.P.)
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 No. 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 specified dangerous mammals and reptiles is also prohibited.

Substances detrimental to the ozone layer (Law No. 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 No. 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.

7.10.2 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 procedures for requesting authorisations from or fulfilling requirements for the public administration;
- paragraph 7.2.2.7 “Management of the procedures regulating 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 the Parent Company, by the other Group companies and/or third-party outsourcers, on the basis of special service agreements.

7.10.2.1 Environment 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 amongst its standards of reference, Intesa San Paolo Group has adopted a specific Environment Policy.
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.

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.

Moreover, part of the sites belonging to the Group have adopted the Environment and Energy Management System in compliance with UNI EN ISO 14001 and UNI CEI EN ISO 50001 whose application is presently being extended.

Control principles

The system set up to monitor the processes described above must be based on the following factors:

- Licensing 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. Internal regulations define the said licensing mechanisms and provide information on the company members to whom such powers have been assigned;
    - 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. More 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 etc.) are separate and distinct from the Structures responsible for consultancy on the evaluation of environment risks and on monitoring the measures suited to prevent and limit the same;
    - 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.

- Monitoring 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 property maintenance/cleaning services (building and persons etc.) with particular attention to the proper keeping of maintenance logs on central heating and refrigeration systems as well as to regular maintenance reports drawn up by the 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.

- Traceability of the process both from an IT standpoint as well as with respect to documentation:
  - Use of IT systems supporting the operations, which ensure registration and archiving of data and information in relation to the purchasing process;
  - Documenting all activities related to the process with particular reference to the proper maintenance logs on central heating systems and on refrigeration in compliance with the provisions of current legislations, particularly with respect to emissions;
  - Preservation, as prescribed by law, (five years from last registration) of the register showing special waste and loading and unloading of hazardous waste;
  - 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 shippers in charge of managing central heating and refrigeration systems;
- Refrain from granting appointments/assignment of work to external consultants and/or suppliers in breach of the documented criteria and objectives of 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 No. 231/2001 and an undertaking to comply therewith;
- Include specific clauses ensuring respect of environment regulations in works agreements, sub-contracting agreements and services supply to persons, buildings, building maintenance, building and plant installation works and other integrated services (e.g. toner supply, management of dispensaries, etc.);
- 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 Managers responsible must first obtain the "product's safety classification " and the CER code to be used for the proper disposal of the same;
- Consider possession of 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).

In any event, it is forbidden to initiate, cooperate/give rise to conduct that could be considered an offence in terms of Legislative Decree No. 231/2001, and, more specifically by mere way of example, to:

- Provide incomplete documentation and/or communicating false or modified data;
- Use deceit which could lead Public Entities in 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.

The Structure Heads involved are obliged to fulfil all the requirements necessary to ensure the efficient and proper 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 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 Anti Bribery corruption policy available at the Bank document repository).