



**SUMMARY OF THE
“ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL OF UBI BANCA S.P.A.
IN ACCORDANCE WITH LEGISLATIVE DECREE No. 231/2001”**

CONTENTS

LEGISLATIVE FRAMEWORK	4
<u>INTRODUCTION</u>	4
<u>THE PREDICATE CRIMES FOR CORPORATE LIABILITY</u>	4
<u>PENALTIES</u>	5
<u>CRIMES COMMITTED ABROAD</u>	5
<u>MODELS OF ORGANISATION, MANAGEMENT AND CONTROL</u>	6
THE UBI BANCA MODEL OF ORGANISATION, MANAGEMENT AND CONTROL PURSUANT TO LEGISLATIVE DECREE NO. 231/2001	7
THE UBI BANCA SUPERVISORY BODY	9
<u>GENERAL PRINCIPLES CONCERNING THE CREATION AND APPOINTMENT OF THE SUPERVISORY BODY</u>	9
<u>FUNCTIONS AND POWERS OF THE SUPERVISORY BODY</u>	9
<u>VERIFICATIONS AND MONITORING THE MODEL</u>	11
<u>DISCLOSURE OBLIGATIONS TO THE SUPERVISORY BODY – LINES OF REPORTING AND REPORTS RECEIVED</u>	11
<u>REPORTING BY THE SUPERVISORY BODY TO GOVERNING BODIES</u>	12
DISCIPLINARY SYSTEM	13
<u>FUNCTION OF THE DISCIPLINARY SYSTEM</u>	13
<u>MEASURES WITH REGARD TO EMPLOYEES</u>	13
<u>MEASURES WITH REGARD TO MEMBERS OF THE BOARD OF DIRECTORS</u>	13
<u>MEASURES WITH REGARD TO COMMERCIAL PARTNERS, AGENTS, FINANCIAL ADVISORS, CONSULTANTS, ASSOCIATES</u>	14
TRAINING AND COMMUNICATION	14
<u>INTRODUCTION</u>	14
<u>INFORMATION PROVIDED TO EMPLOYEES AND MEMBERS OF THE GOVERNING BODIES</u>	14
<u>INFORMATION PROVIDED FOR OTHER RECIPIENTS</u>	15
<u>TRAINING ACTIVITY</u>	15
ACTIVITIES IDENTIFIED AS SENSITIVE FOR THE PURPOSES OF LEGISLATIVE DECREE NO. 231/2001 IN UBI BANCA	15
<u>THE ACTIVITIES IDENTIFIED AS SENSITIVE FOR THE PURPOSES OF DECREE 231 IN UBI BANCA WITH REGARD TO CRIMES AGAINST PUBLIC ADMINISTRATIONS</u>	15
<u>THE ACTIVITIES IDENTIFIED AS SENSITIVE FOR THE PURPOSES OF DECREE 231 IN UBI BANCA, WITH REGARD TO THE FORGERY OF COINS, PUBLIC CREDIT NOTES, DUTY STAMPS, IDENTIFICATION INSTRUMENTS AND DISTINCTIVE SIGNS</u>	16
<u>THE ACTIVITIES IDENTIFIED AS SENSITIVE FOR THE PURPOSES OF DECREE 231 IN UBI BANCA WITH REGARD TO CORPORATE CRIMES</u>	17
<u>THE ACTIVITIES IDENTIFIED AS SENSITIVE FOR THE PURPOSES OF DECREE 231 IN UBI BANCA WITH REGARD TO CRIMES OF TERRORISM AND SUBVERSION OF DEMOCRATIC LAW</u>	18
<u>THE ACTIVITIES IDENTIFIED AS SENSITIVE FOR THE PURPOSES OF DECREE 231 IN UBI BANCA WITH REGARD TO CRIMES AGAINST THE PERSON OF INDIVIDUALS</u>	19
<u>THE ACTIVITIES IDENTIFIED AS SENSITIVE FOR THE PURPOSES OF DECREE 231 IN UBI BANCA WITH REGARD TO THE CRIME OF MARKET RIGGING AND THE CRIMES (AND CORPORATE OFFENCES) OF ABUSE OF INSIDER INFORMATION AND MARKET MANIPULATION</u>	19
<u>THE ACTIVITIES IDENTIFIED AS SENSITIVE FOR THE PURPOSES OF DECREE 231 IN UBI BANCA WITH REGARD TO TRANSNATIONAL CRIMES</u>	20
<u>THE ACTIVITIES IDENTIFIED AS SENSITIVE FOR THE PURPOSES OF DECREE 231 IN UBI BANCA WITH REGARD TO CRIMES CONCERNING HEALTH AND SAFETY AT THE WORKPLACE</u>	20
<u>THE ACTIVITIES IDENTIFIED AS SENSITIVE FOR THE PURPOSES OF DECREE 231 IN UBI BANCA WITH REGARD TO CRIMES CONSISTING OF THE RECEIPT, LAUNDERING, USE OF MONEY, GOODS OR BENEFITS OF ILLICIT ORIGIN AND “SELF-LAUNDERING”</u>	21
<u>THE ACTIVITIES IDENTIFIED AS SENSITIVE FOR THE PURPOSES OF DECREE 231 IN UBI BANCA WITH REGARD TO COMPUTER CRIMES AND THE ILLICIT PROCESSING OF DATA</u>	22
<u>THE ACTIVITIES IDENTIFIED AS SENSITIVE FOR THE PURPOSES OF DECREE 231 IN UBI BANCA WITH REGARD TO ORGANISED CRIME</u>	23
<u>THE ACTIVITIES IDENTIFIED AS SENSITIVE FOR THE PURPOSES OF DECREE 231 IN UBI BANCA WITH REGARD TO CRIMES AGAINST INDUSTRY AND COMMERCE</u>	24

<u>THE ACTIVITIES IDENTIFIED AS SENSITIVE FOR THE PURPOSES OF DECREE 231 IN UBI BANCA WITH REGARD TO THE VIOLATION OF COPYRIGHT.</u>	24
<u>THE ACTIVITIES IDENTIFIED AS SENSITIVE FOR THE PURPOSES OF DECREE 231 IN UBI BANCA WITH REGARD TO ENVIRONMENTAL CRIMES.</u>	25
<u>THE ACTIVITIES IDENTIFIED AS SENSITIVE FOR THE PURPOSES OF DECREE 231 IN UBI BANCA WITH REGARD TO THE EMPLOYMENT OF CITIZENS OF THIRD PARTY COUNTRIES WHOSE STAY DOCUMENTS ARE IRREGULAR.</u>	25
THE SYSTEM OF CONTROLS	25

Legislative framework.

Introduction.

Legislative Decree No. 231 of 8th June 2001 (hereinafter “Decree 231”) lays down the rules for the “liability of entities for corporate offences resulting from crimes”.

More specifically those rules apply to legal entities, companies and associations even if they have no official legal status.

According to the rules introduced by Decree 231, companies can in fact be held “liable” in relation to certain crimes actually committed or attempted, where they have been carried out in the interest of or to the advantage of the entity itself by senior officers of the company and/or by those who are subject to their management or supervision.

An entity is not liable if the persons indicated acted solely in their own interests or those of third parties (Art. 5, paragraph 2, of Decree 231).

The corporate liability of entities is independent of the criminal responsibility of the individuals who have committed the crimes and it accompanies the latter.

Liability for corporate offences resulting from crime is normally ascertained as part of the same criminal proceedings relating to the natural person who is charged with committing the crime.

Decree 231 introduced new elements to Italian law because penalties of both a monetary nature and consisting of prohibitions in relation to crimes committed by persons functionally related to entities are now applicable to those entities.

Entities are nevertheless excluded from corporate liability if, amongst other things, an entity has adopted and effectively implemented models of organisation, management and control designed to prevent crimes, before they are committed. These models can be adopted on the basis of codes of conduct (guidelines) drawn up by associations which represent the entity, including the Italian Banking Association, and which have been communicated to the Ministry of Justice.

The predicate crimes for corporate liability.

The offences (criminal and administrative) for which an entity may be held responsible according to Decree 231 can be comprised, for easy perusal, within the following categories:

- crimes against public administrations (referred to in articles 24 and 25 of Decree 231);
- computer crime (referred to in article 24-*bis* of Decree 231);
- organised crime (referred to in article 24-*ter* of Decree 231);
- crimes against public trust (referred to in article 25-*bis* of Decree 231);
- crimes against industry and commerce (referred to in article 25-*bis*.1 of Decree 231);
- corporate crimes (referred to in Art. 25-*ter* of Decree 231);
- crimes of terrorism and subversion of democratic law (referred to in article 25-*quater* of Decree 231);
- crimes concerning customs of mutilation of female genital organs (referred to in article 25-*quater*.1 of Decree 231);
- crimes against the person of the individual (mentioned in article 25-*quinquies* of Decree 231);
- corporate offences concerning market abuse (referred to in Art. 25-*sexies* of the Decree 231 and article 187-*quinquies* of the Consolidated Finance Law);

- transnational crimes referred to in Art. 10 of Law No. 146 of 16th March 2006 which “ratifies and implements the United Nations convention and protocols on transnational organised crime, adopted by the General Assembly on 15th November 2000 and 31st May 2001”;
- crimes committed in violation of health and safety regulations at the work place (referred to in article 25 *septies* of Decree 231);
- crimes consisting of the receipt, laundering and use of money, goods or benefits of illicit origin, and also money-laundering (referred to in article 25-*octies* of Decree 231);
- crimes concerning the violation of copyright (referred to in article 25-*novies* of Decree 231);
- the crime of “inducing persons not to make statements or to make false statements to judicial authorities” (referred to in article 25-*novies* of Decree 231).
- environmental crimes (referred to in article 25-*undecies* of Decree 231).
- the crime of “employing citizens of third party countries whose stay documents are irregular”(referred to in article 25-*duodecies* of Decree 231)
- crimes of racism and xenophobia (referred to in Art. 25-*terdecies* of Decree 231).

Penalties.

The following penalties are provided for by Decree 231 for entities as a consequence of committing or attempting to commit the aforementioned crimes:

- penalties of a prohibition nature (applicable even as a precautionary measure) of a duration of not less than three months and not more than two years, which may consist of:
 - disqualification from carrying on a business;
 - suspension or revocation of authorisations, licences or concessions relating to the offence committed;
 - exclusion from contracts with public administrations;
 - exclusion from entitlement to public concessions, grants, contribution or subsidies and the revocation of those granted;
 - prohibition on advertising goods or services;
- confiscation of the profits of the crime;
- publication of the ruling.

Fines are decided by the criminal judge by using a system based on “quotas”, which are not less than one hundred and not greater than one thousand in number and which are variable in amount for each single quota, varying from a minimum of €258.23 to a maximum of €1,549.37 (and therefore for an amount which ranges from a minimum of €25,823,00 and a maximum of €1,549,370.00).

An entity is deemed liable even in cases of attempted crimes, which to say in cases where actions have been carried out designed unequivocally to commit one of the crimes which constitute predicate offences by the legal entity.

In these cases fines (in terms of amount) and prohibition penalties (in terms of time) are reduced by between one third and one half, while no penalties are imposed in cases where the entity voluntarily prevents the deed from being accomplished or the event from occurring (Art. 26 of Decree 231).

Crimes committed abroad.

In accordance with Art. 4 of Decree 231, an entity may be held liable in Italy for crimes relevant for the purposes of the corporate liability of entities that are committed abroad. The Illustrative Report on Decree 231 underlines the need to prevent a type of criminal situation which frequently occurs from going unpunished and also to prevent the entire legislation in question from being easily evaded.

Models of organisation, management and control.

Decree 231 attributes the value of extenuating circumstances to the models of organisation, management and control of entities. More specifically, if a crime is committed by a person in a 'senior' position, the entity is not held liable if it can prove that:

- a) the governing body adopted and effectively implemented, before the fact was committed, appropriate models of organisation and management designed to prevent crimes of the type committed;
- b) the task of supervising the functioning and compliance with the models and updating them has been assigned to a body of the entity with independent powers to act and monitor;
- c) the persons who committed the crime fraudulently evaded the models of organisation and control;
- d) there was no omission or insufficiency of supervision by the supervisory body.

If, however, a crime is committed by persons subject to the management or supervision of others, an entity is held liable if the crime committed was made possible by the violation of management or supervision obligations which the entity is held to comply with.

In any event, the violation of management or supervision obligations is excluded if an entity has adopted and effectively implemented, before the deed was committed, appropriate models of organisation and management designed to prevent crimes of the type committed.

Art. 7, paragraph 4 of Decree 231 also defines the requirements for effective implementation of organisational models and requires the following:

- periodic verification of the model and modification of it when significant violations of regulations are discovered or when organisational and business changes occur;
- an appropriate disciplinary system which punishes failure to comply with the regulations of the model.

In the hypothesis of the case contemplated by the cited article 7, the onus of proof concerning the adoption of Model 231 lies with the Public Prosecutor.

Decree 231 describes the contents of the models of organisation and management and state that in relation to the extension of powers delegated and the risk of crimes being committed, these must:

- identify the areas of activities in which crimes may be committed;
- create specific regulations to programme the formation and implementation of an entity's decision regarding the prevention of criminal offences;
- identify ways of managing funds in order to prevent crimes from being committed;
- establish compulsory reporting to the body responsible for supervising the functioning of models and compliance with them;
- introduce a disciplinary system which punishes failure to comply with the regulations of the model.

Furthermore, in accordance with Art. 30 of Legislative Decree No. 81/2008 (hereinafter also the "Consolidated Safety Law"), a model of organisation and control which effectively exempts an entity from corporate liability pursuant to Decree 231 must be adopted and effectively implemented, ensuring the existence of a corporate system which satisfies all the legal requirements concerning the following:

- a) compliance with legal technical and structural standards relating to equipment, plant, workplaces, and chemical, physical and biological agents;
- b) risk assessment activities and implementation of the resulting preventative and protection measures;
- c) activities of an organisational nature, such as emergencies, first aid, contract management, periodic safety meetings and consultation with workers' safety representatives;
- d) health and hygiene supervisory activities;

- e) the provision of information and training for workers;
- f) oversight activities relating to compliance with operational safety procedures and instructions by workers;
- g) the acquisition of documentation and certifications that are compulsory by law;
- h) periodic verification of the application and effectiveness of the procedures adopted.

The model must also provide for the following:

- appropriate systems to record the implementation of the activities listed above;
- with regard to the requirements concerning the nature and dimensions of the organisation and the type of activity performed, the functions must be organised in such a manner as to ensure they have the expertise and powers needed to verify, assess, manage and control risks;
- an appropriate disciplinary system which punishes failure to comply with the regulations of the model;
- an appropriate system to monitor implementation of the model and maintenance of the appropriateness of the measures adopted over time;
- review and modification of the model when significant violations of accident prevention and safety at work regulations occur, or when organisational changes and scientific and technological progress occur.

The adoption and effective implementation of a 231 Model detects, even after the crime has been committed, can detect with a view to mitigating the consequences provided for by Decree 231 in accordance with articles 12, 17 and 78.

As concerns the crimes listed in Art. 25 of Decree 231 in particular, a further mitigating circumstance exists for prohibition penalties in cases where, before the conviction in the court of first instance (and therefore not according to the general rule that is applied until a hearing commences), the entity has effectively taken steps: to prevent the criminal activity from leading to further consequences; to secure the proofs of the crimes and to identify those responsible; or to confiscate sums or other benefits and eliminate organisational shortcomings which have determined the crime by the adoption and implementation of organisational models designed to prevent crimes of that type from occurring again.

The UBI Banca model of organisation, management and control pursuant to Legislative Decree No. 231/2001.

UBI Banca has adopted its own “231” model of organisation, management and control, which complies with Decree 231 and the relative legislation and regulations that apply and is based on principles that are already rooted in its governance culture and on the recommendations contained in the Italian Banking Association Guidelines.

This 231 Model of Organisation, Management and Control of UBI Banca is composed of the following list of documents:

- (i) the general part of the Model which gives a description of the relative regulatory framework;
 - the reality of the company (system of governance and organisational structure of UBI Banca);
 - the structure of the Model;
 - identification and appointment of the supervisory body of UBI Banca, with specification of the relative powers, tasks and reporting systems;
 - the functioning of the disciplinary system and the relative penalties;

- the training and communication plan to be adopted to ensure that people have a knowledge of the measures and regulations of the model;
- (ii) the special part of the Model, which gives a description of:
 - the types of crime (and corporate offences) that are important for the purposes of the corporate liability of entities which the Bank had decided to take into consideration in view of the nature of its business;
 - sensitive processes/activities and the relative control procedures.

(iii) a Code of Conduct, which constitutes UBI Banca’s internal self-disciplinary rulebook, which has been drafted on the basis of the Code of Ethics. It provides those whom it governs with a framework of the principles of behaviour with which to assess concrete situations from time-to-time and whether decisions to be taken are compliant with ethical principles and with regulations.

(iv) a Code of Ethics, which defines the manner in which UBI Banca intends to pursue its mission and act in dealings with its various stakeholders, by basing its management and operating activities on observance of moral and legal obligations towards society.

(v) an MIAR (Risk Area Identification Matrix – RAIM), which, as specified later in this document, maps activities, which in consideration of the specific contents, are potentially vulnerable to the commission of crimes (and corporate offences) that are significant for the purposes of the possible corporate liability of UBI Banca.

(vi) an Implementation Matrix which specifies the relationships between the RAIM and the relative protocols for implementing the provisions of the 231 Model.

(vii) the 231 Regulation which, in compliance with the recommendations contained in section 3 of the 231 Model (“Model of Organisation, Management and Control of UBI Banca S.p.A.”) and section 4 (“Supervisory Body pursuant to Decree 231”), has the purpose of setting out the following:

- the role of the Parent in relation to its subsidiaries for the purposes of Decree 231;
- the process for updating the 231 Model, by formulating proposals for amendments for submission to be submitted to the Board of Directors for approval;
- the process for verification of the adequacy of 231 Model for the purpose of evaluating its ability to prevent illegal conduct and evaluate the consistency of the actual behaviour within UBI Banca with the provisions of the 231 Model itself;
- the establishment of a standardised and predetermined system for the exchange of information.

The documentation which UBI Banca possesses to describe its organisational structure and to govern its operations, inclusive of activities that are sensitive for the purposes of the 231 Model, also includes the following:

- a Code of Ethics, which defines the general ethical principles and rules of conduct for relations with stakeholders on which the management style of the bank is based;
- a Code of Conduct, drafted on the basis of the Code of Ethics, which represents UBI Banca’s internal self-regulatory code and provides a framework of the principles of behaviour with which to assess concrete situations from time-to-time and whether decisions to be taken are compliant with ethical principles and with regulations;

- the 231 Model which identifies areas at risk of the possible commission of crimes and corporate offences and the relative controls. It also establishes a Supervisory Body responsible for monitoring its adoption and constant implementation;
- the UBI Banca Group’s Model Policy and Regulation which defines relations between the Governing Boards and the Senior Management of the Parent and the Governing Boards and Senior Management of the companies that form part of the Group;
- the General Company Regulation which governs the interaction of governing bodies with the units of the Parent;
- catalogue of sources used for the regulatory framework;
- catalogue of documents that must be signed by personnel;
- Internal Regulations, which supplement the external regulations in force for banking and financial intermediaries.

The UBI Banca supervisory body.

As already said, on the basis of the provisions of Decree 231 (Art. 6, paragraph 1, letters a) and b) an entity may be exonerated from liability resulting from the commission of crimes by the persons specified under Art. 5 of Decree 231, if the management body has, in addition to having adopted and implemented an appropriate organisation model of organisation, also entrusted the task of supervising the functioning and compliance with the models and updating them to a body of the entity with independent powers to act and monitor.

Entrusting the aforementioned tasks to a body with independent powers to act and monitor together with proper and effective performance of those activities represent therefore necessary and indispensable assumptions for exoneration of an entity from liability as provided for by Decree 231.

UBI Banca has designated the following as its 231/01 Supervisory Body (hereinafter the “**Supervisory Body**”): (i) a mixed collegiate body composed of a minimum of three and a maximum of five members; (ii) it is comprised mainly of members external to the Bank; (iii) it possesses the qualities of professionalism and expertise in the banking, financial, economic and risk control areas, amongst others.

General principles concerning the creation and appointment of the Supervisory Body

UBI Banca’s Supervisory Body is nominated by a resolution of the Board of Directors and its term of office is three years.

Functions and powers of the Supervisory Body

The Supervisory Body is granted the following duties and powers to act and monitor required to ensure effective and efficient supervision of the functioning of and compliance with the Model in accordance with the provisions of Art. 6 of Decree 231:

- a) to verify, on the basis of a work plan approved annually, the effectiveness of the Model in relation to the organisation of the Bank and its effective ability to prevent the commission of crimes pursuant to the Decree, and it makes proposals, where considered necessary, to update the 231 Model with particular attention paid to developments and changes in the Bank’s organisational structure, its operations and/or in the current regulatory framework;
- b) to monitor, on the basis of the work plan approved, the validity of the 231 Model and of its procedures (“protocols”) over time, and it undertakes, subject at times to prior consultation with the organisational units involved, all actions necessary to ensure its effectiveness;

- c) to carry out, on the basis of the work plan approved, or also by means of unprogrammed surprise inspections, on-site controls of organisational units considered at risk of crime, in order to ascertain whether activities are being carried out in compliance with the 231 Model adopted;
- d) to verify the adoption and effective functioning of solutions proposed by means of follow-up activities;
- e) to conduct, by means of special action programmes, verification of actions carried out by persons in possession of powers to sign;
- f) to periodically verify, with support from other competent functions, the system of powers in force, and to recommend modifications where operational powers and/or the rank in question do not correspond to the powers to represent the Bank conferred on internal managers or the managers under them;
- g) to define and oversee, in implementation of the Model, the lines of reporting that allow the Supervisory Body to be constantly kept up-to-date by the organisational units concerned involved in activities considered at risk of crime and also to establish communication and reporting procedures in order to acquire knowledge of potential violations of the Model;
- h) to oversee the effective application of the 231 Model and to detect any changes in behaviour which might potentially emerge from an analysis of information flows and reports received;
- i) to implement, in compliance with the 231 Model, effective reporting to the competent governing bodies which allows the Supervisory Body to inform them of the efficacy of the Model and compliance with it;
- j) to promptly inform the Board of Directors of any violations of provisions (regulatory and procedural) which might give rise to crimes pursuant to the 231 Decree;
- k) to encourage, in collaboration with the competent functions, activity to inform and train staff by means of appropriate initiatives to disseminate knowledge and understanding of the 231 Model and to verify that these are actually carried out;
- l) to monitor internal managers of areas at risk of crime to ensure that they are properly trained on their tasks and duties relating to oversight of their area for the purposes of preventing the commission of crimes pursuant to the Decree;
- m) to communicate any violations of the Model to the competent bodies for the purposes of taking possible disciplinary measures and also to monitor the outcome of these;
- n) to verify and evaluate the appropriateness of the disciplinary system within the meaning of and in compliance with Decree 231;
- o) to provide guidelines for the supervisory bodies of subsidiaries and oversee their distribution.

For the purposes of carrying out its duties, the following powers have been conferred on the Supervisory Body:

- a) to access all documents and/or company information of importance for carrying out the functions assigned to the Supervisory Body in accordance with Decree 231 and the 231 Model;
- b) to make use of outside advisors of proven professionalism in cases in which this becomes necessary to carry out the activities for which it is responsible;
- c) to demand that managers of organisational units promptly provide information, data and/or news requested of them;
- d) to proceed, should it be necessary, to hear directly from employees, directors and/or members of the Bank's Management Control Committee;
- e) to dispose of its own independent budget which the Supervisory Body itself indicates

to the Board of Directors in order for it to approve the necessary resolution;

- f) to request information from external consultants, agents, financial and commercial partners, service providers and also auditors of accounts with regard to activities carried out on behalf of the Bank.

The Supervisory Body shall avail itself of a secretary, selected by the Supervisory Body from amongst its members or from amongst employees of the Bank, who shall be responsible for managing support activities for the preparation of meetings (i.e. convening meetings, acquiring and assessing material to be examined by the Supervisory Board), minuting meetings, recording minutes in company records and storage of those records.

In order to better carry out its duties and its functions, the Supervisory Board may avail itself, to carry out its operating activities, of the Internal Audit, Legal, Compliance and Organisation Functions of UBI and also of other organisational units which may be of use to it, from time to time, in carrying out its activities. As concerns issues regarding health and safety at the workplace in particular, the Supervisory Body may avail itself of all the staff involved in the management of the relative aspects (*RSPP* - Manager of the Prevention and Protection Service, *ASPP* – Prevention and Protection Service staff, *RLS* – workers’ safety representatives, *MC* - corporate physician, first aid qualified staff, firefighting qualified staff).

The Supervisory Board adopts its own regulation in order to govern the procedures of its functioning.

Verifications and monitoring the model.

The Supervisory Body prepares a supervision work plan with which it plans its activities which contains the following: a calendar of activities to be carried out during the year; frequencies with which controls are carried out; identification of analysis criteria and procedures; possibility of carrying out unprogrammed inspections and controls.

The Supervisory Body is granted wide ranging powers during checks and inspections in order for it to perform the tasks assigned to it effectively and in particular it shall be given access, with no limitation whatsoever, to corporate documents and be able to carry out interviews, acquire information from third parties and make use of advisors specially appointed for the purpose.

Disclosure obligations to the Supervisory Body – Lines of reporting and reports received.

Employees are required to inform the Supervisory body of possible violations of the 231 Model and/or of conduct non-compliant with its provisions, by means of the following channels of communication:

- **email:** Organismo.di.Vigilanza.231@ubibanca.it
- **letter to the address:** Unione di Banche Italiane S.p.A.
Organismo di Vigilanza 231
Piazza Vittorio Veneto, 8
24122 – Bergamo

Reporting obligations regarding conduct contrary to the provisions of the 231 Model fall within the broader duty of diligence and the obligation of loyalty towards an employer pursuant to articles 2104 and 2105 of the Italian Civil Code. Reports must be made in written form and may be anonymous.

“Whistleblowing” reports of suspect or proven violations of the 231 Model are also of importance for the aforementioned purposes, to be made by following the procedures adopted by the Bank in implementation of the applicable legislation and regulations in force from time-to-time.

The following rules of a general nature apply in this respect:

- violation of the 231 Model is defined as any conduct which violates the principles of the 231 Model inclusive of procedures that constitute its implementation;
- all senior officers of the Bank are required to promptly report any information regarding: i) crimes committed or the reasonable danger of crimes (and corporate offences) relevant for the purposes of the corporate liability of entities being committed; ii) “practices” not in line with the codes of conduct issued by the Bank; iii) behaviour which might, in any case determine a violation of the 231 Model;
- each manager of an organisational unit with responsibility for the co-ordination units is required to officially and promptly report any behaviour that is not compliant with the 231 Model to the Supervisory Board;
- employees, agents, commercial partners, consultants, associates, financial advisors, those termed ‘para-employees’ and all stakeholders in general report violations (or presumed violations) of the 231 Model with regard to business with UBI Banca and activity performed with regard to UBI Banca to the Supervisory Body in accordance with the provisions laid down in sub-section 4.5.1 of this document;
- the Supervisory Body assesses, using its own discretion and under its own responsibility, the reports received and it identifies any necessary initiatives;
- if a report of violations of the 231 Model concerns members of the Board of Directors, it will also be communicated to the Chairman of the Board of Directors or, if it concerns the latter, to the Chairman of the Management Control Committee.

The Supervisory Body assesses reports received, inclusive of anonymous reports in accordance with the provisions of the 231 Model.

Information concerning the following must also be communicated to the Supervisory Body by the corporate functions that work in the area of sensitive activities: i) the periodical results of control activities put in place by it to implement the 231 Model (summary reports of activities performed, monitoring activities, indexes of actual performance etc.); ii) anomalies or unusual occurrences encountered in the information available (a fact which may not be important considered by itself, could be evaluated differently if it repeats or happens also in other areas).

All the information, documentation and reports acquired in carrying out institutional duties must be filed and kept for at least five years by the Supervisory Body, with care taken to maintain the confidentiality of the documents and information acquired in compliance, amongst other things, with regulations on privacy.

Persons making reports in good faith are guaranteed against any form of retaliation, discrimination or penalty and in any case the confidentiality of the identity of the person making the report is guaranteed unless legal obligations and protection of the rights of the Bank or of persons mistakenly and/or maliciously accused do not allow it.

Reporting by the Supervisory Body to governing bodies.

The Supervisory Body reports on the implementation of the model, any critical aspects there may be and the need to make modifications to it.

Two separate lines of reporting are provided for:

- the first is on a continuous basis directly to the Chief Executive Officer and the General Manager;
- the second is periodic to the Board of Directors and to the Management Control Committee.

Disciplinary system.

Function of the disciplinary system.

The definition of an adequate disciplinary system constitutes an essential necessary condition if the model of organisation, management and control in accordance with Decree 231 is to constitute a justification with regard to the corporate liability of entities.

Measures with regard to employees.

Observance of the regulations and rules of conduct specified under the 231 Model constitutes compliance by the employees of the UBI Banca with the obligations contained in Art. 2104, paragraph 2 of the Italian Civil Code, obligations of which the content of the Model represents a substantial and integral part.

Violation of the individual regulations and rules of the 231 Model by employees of UBI Banca always constitutes a disciplinary offence.

The measures laid down in the 231 Model that it is intended to punish if violated, are communicated by means of an internal memorandum to all employees and are placed on display in places accessible to all and they are binding on all employees of the Bank.

Disciplinary measures are imposed on employees of UBI Banca, in accordance with Art 7 of Law No. 300 of 20th May 1970 (the “Workers’ Statute”) and any specific legislation that may apply.

As concerns penalties resulting from violations of the regulations of the 231 Model, the general principles and rules contained in the disciplinary code already issued by UBI Banca and communicated in the same manner as described above apply.

For employees who are not senior managers, these measures are those contained in the disciplinary regulations of the relative national trade union agreement.

Disciplinary action is taken for each report of a violation of the 231 Model in order to ascertain whether a violation has actually taken place. For the ascertainment of infringements, the disciplinary procedures and the imposition of penalties, the powers conferred on the management of the UBI Banca within the limits of the respective authorisations and responsibilities apply.

However, each action concerning these procedures must be communicated to the Supervisory Body which will assess where responsibility lies.

UBI Banca nevertheless reserves the right to claim compensation for damages caused by violation of the model by an employee.

If the regulations and rules of conduct contained in the 231 Model are violated by senior managers, once UBI Banca has ascertained the responsibility of the person committing the violation, it adopts those measures it considers most appropriate. If the violation of the 231 Model determines the loss of a relationship of trust between the Bank and a senior manager, the penalty is dismissal for just cause.

Measures with regard to members of the Board of Directors.

Special penalties are employed if violations of the regulations and rules of conduct of the 231 Model are committed by members of the Board of Directors.

Measures with regard to commercial partners, agents, financial advisors, consultants, associates.

The violation by commercial partners, agents, financial advisors, consultants, external associates, or others with whom the Bank has entered into contracts, of the regulations and rules of conduct contained in the 231 Model that apply to them or crimes (and corporate offences) relevant for the purposes of the corporate liability of entities committed by them are punished on the basis of the specific clauses contained in the relative contracts.

Clearly, UBI Banca nevertheless reserves the right to claim compensation for damages caused by violation of the regulations and rules of conduct contained in the 231 Model by these external parties described above.

Training and communication.

Introduction

In order to implement the Model effectively, UBI Banca intends to ensure adequate communication of its contents both inside and outside its organisation.

More specifically, it is the objective of UBI Banca to extend communication of the contents of the Model, not just to its own employees, but also to those who, although not officially employees, work, even on a casual basis, to achieve the objectives of UBI Banca as a result of contractual relationships.

The activity of communication and training, which differs according to the recipients, is in any case characterised by principles of completeness, clarity, accessibility and continuity in order to allow the various recipients full knowledge of the Bank's regulations which they are held to comply with and the ethical standards which must guide their behaviour.

Communication and training activity is supervised and supplemented by the Supervisory Body.

Information provided to employees and members of the governing bodies.

Each employee is required to: i) acquire a knowledge of the contents of the 231 Model; ii) know the operating procedures with which their activity must be performed; iii) contribute actively in relation to their position and their responsibilities to the effective implementation of the 231 Model, reporting any failures encountered in it.

In order to guarantee effective and rational communication, UBI Banca promotes and facilitates acquisition of a knowledge of the contents of the 231 Model by employees, where the depth of the knowledge differs according to the degree of involvement in the activities identified as sensitive according to Decree 231.

The 231 Model may be consulted by employees on the corporate intranet. Furthermore, in order to facilitate understanding and knowledge of the 231 Model, employees are required to participate in specific training initiatives provided by the Bank which shall differ according to their degree of their involvement in activities identified as sensitive according to Decree 231.

New employees shall receive a copy of the 231 Model and they shall be required to sign a declaration stating that they shall comply with the contents of the 231 Model as described in it.

The same procedures for the communication of the 231 Model used for employees shall apply to members of the governing bodies of UBI Banca.

Appropriate instruments of communication shall be adopted to update employees on any modifications that may be made to the 231 Model and on changes in procedures, regulations or organisation.

Information provided for other recipients.

Communication activity and the contents of the 231 Model is also addressed to those external parties who work for UBI Banca under contracts or who represent the Bank but without being bound to subordination to it (e.g. commercial partners, agents and consultants, financial advisors, distributors, sales persons and other independent associates). To achieve this the most important external associates of UBI Banca will be furnished with a copy of this document and a copy of the Code of Ethics. Third parties in receipt of those documents shall be required to sign a declaration stating that they have received the documents and agree to comply with the contents of them.

Having considered the purposes of the 231 Model, UBI Banca shall consider the advisability of communicating the contents of the 231 Model to outside parties other than those indicated for the sake of example and more generally to markets.

Training activity.

UBI Banca performs specific training activity, with the support of its internal training functions, for all employees in order to ensure that there is widespread and adequate knowledge and understanding of the Model. It is also designed to encourage the diffusion of a corporate culture which is oriented towards the pursuit of increasingly greater transparency and integrity.

The following methods of training are used:

- classroom sessions with dedicated lessons or by the introduction of specific modules in other training sessions depending on the contents and the recipients of the training, with tests to verify the level of learning;
- e-learning: with a module on the general part for all employees, with intermediate exercises and learning tests.

The contents of training activities are constantly updated on the basis of updates to the 231 Model itself.

Participation in training activities is compulsory. Acting through the organisational units responsible, the supervisory body collects and archives evidence and certification of actual participation in this training activity.

Activities identified as sensitive for the purposes of Legislative Decree No. 231/2001 in UBI Banca

The activities identified as sensitive for the purposes of Decree 231 in UBI Banca with regard to crimes against public administrations.

An analysis of the corporate processes of UBI Banca identified the areas in which the types of crimes mentioned in articles 24, 25 and 25 *decies* of Decree 231 may theoretically be committed. A list of the activities considered “sensitive” or at risk with regard to crimes against public administrations is given below, as examples but not limited to these, as follows:

1. negotiation, signing and performance of contracts/conventions with public entities by means of negotiated procedures (direct award or private negotiation) or public procedures (open or restricted);
2. activities performed by the Bank when appointed to perform a public service (e.g. provision of treasury services for public administrations; tax payment services; the distribution of government debt instruments);
3. management of approval procedures, disbursement activities and the relative administrative formalities relating to the grant of loans and/or guarantees, inclusive of those which benefit from government subsidies and/or guarantees;

4. management of relations with public entities concerning property rights (land office and land register, etc.);
5. management of relations with public sector entities – including public supervisory authorities (e.g. the Bank of Italy; the Financial Intelligence Unit, Consob (Italian securities market authority), the Antitrust Authority, Authority for Electricity and Gas, Authority to Guarantee Communications, IVASS (insurance authority), Covip (pensions authority), Authority to Guarantee the Protection of Personal Data) – which operate as public authorities active in determined areas of responsibility. Compliance and inspections;
6. management of relations with public entities to obtain authorisations and licences for carrying on company business, or more generally in the interest and to the advantage of the bank;
7. selection, appointment and management of personnel, including personnel belonging to protected groups or for whom concessions are granted for employing them;
8. relations with the judicial authorities and its ancillaries (e.g. the magistrates, the judicial police, etc.);
9. the management of relations with members of governing bodies, employees or third parties involved in court proceedings;
10. the implementation and/or promotion and management of sponsorships and commercial or humanitarian and charitable initiatives;
11. management of relations with the financial authorities, also for tax compliance purposes;
12. acquisition and/or management of contributions/subsidies/loans granted by public entities to the Bank;
13. management of litigation in- and out-of-court (e.g. civil, tax, labour law, administrative law, criminal law, credit recovery etc.). The appointment of lawyers and the co-ordination of their activities;
14. the negotiation, signing and performance of agency, intermediation, financial advisor and brokerage contracts (selection, creation and regulation of relations, setting fees, management and termination of relations);
15. the management of funds and powers to sign;
16. the sale and purchase, lease and management of real estate properties;
17. negotiation and grant of exceptions to conditions on banking or financial products and services;
18. definition, management and grant of free gifts and use of company property.

The activities identified as sensitive for the purposes of Decree 231 in UBI Banca, with regard to the forgery of coins, public credit notes, duty stamps, identification instruments and distinctive signs.

An analysis of the corporate processes of UBI Banca identified an area in which the types of crimes mentioned in article 25-bis of Decree 231 may theoretically be committed. As examples, but not limited to these, a list of the activities considered sensitive or at risk with regard to the crimes of the forgery of coins, public credit notes, duty stamps, identification instruments and distinctive signs is given below as follows:

1. management and availability, use or holding of cash /duty stamps;
2. relations with suppliers as concerns outsourcing cash-handling activities;
3. the conception, reproduction, creation or use for commercial of industrial purposes of brands, distinctive marks, drawings or industrial models;
4. the introduction into the territory of the State and the storage for sale or distribution on the retail market of intellectual property or industrial products with brands or distinctive national or foreign marks;
5. management, procurement and custody of gold that is owned;

6. deposit and management of deposits of gold belonging to third parties;
7. management of operations to purchase and sell gold with customers or partner banks.

The activities identified as sensitive for the purposes of Decree 231 in UBI Banca with regard to corporate crimes.

An analysis of the corporate processes of UBI Banca identified an area in which the types of crimes mentioned in article 25-ter of Decree 231 may theoretically be committed. A list of the activities considered “sensitive” or at risk identified with regard to corporate crimes is given below, as examples but not limited to these, as follows:

1. preparation of accounts (inclusive of consolidated accounts), reports and other company communications required by law for disclosure to shareholders or the public and compliance with obligations introduced by Law No. 262/2005 concerning company accounting documents;
2. preparation of prospectuses required for the sale to the public of financial products and/or for admission for listing on regulated markets or documents to be published for public tender offers to purchase, sell or swap shares or other similar prospectuses and so forth;
3. management of relations with the Board of Directors, independent auditors and shareholders; Preparation, keeping and archiving of the documents over which they could exercise control;
4. operations concerning own shares and quotas and operations concerning share capital and allocation of profits;
5. activities to prepare general meetings of shareholders, the proceedings and minutes of general meetings;
6. communications to the supervisory authorities of the banking sector and other supervisory authorities and management of relations with them;
7. communication of conflicts of interest in compliance with Art. 2391, paragraph 1, of the Italian Civil Code;
8. winding up of companies;
9. management of intercompany transactions;
10. the authorisation and provision of banking, financial and/or investment services;
11. the authorisation and provision of insurance services;
12. the management of investments other than banking and financial services (e.g. the acquisition of companies or stakes in companies, strategic agreements, other extraordinary finance transactions);
13. the negotiation, signing and performance of agency, intermediation, , financial advisor and brokerage contracts (selection, creation and regulation of relations, setting fees, management and termination of relations);
14. management of approval procedures, disbursement activities and the relative administrative formalities relating to the disbursement of finance (inclusive of that which benefits from government subsidies);
15. management of intragroup activities that are either delegated or managed in service;
16. definition, management and grant of free gifts and use of company property;
17. the implementation and/or promotion and management of sponsorships and commercial or humanitarian and charitable initiatives;
18. negotiation and grant of exceptions to conditions on banking or financial products and services;
19. relationships that the Bank holds with stakeholders and external counterparties;
20. negotiation (by means of private negotiations or the organisation of public tenders) and management of relationships with consultants or suppliers of goods and/or services (management of the procurement process);

21. negotiation (by means of private negotiations or the organisations of public tenders) and management of relationships with external counterparty customers relating to revenue account processes, also in relation to standing commercial agreements;
22. management of career paths and of financial/career rewards;
23. management of litigation in and out of court (e.g. civil, tax, labour law, administrative law, criminal law, credit recovery etc.). The appointment of lawyers and the co-ordination of their activities;
24. selection, appointment and management of personnel, including personnel belonging to protected groups or for whom concessions are granted for employing them;
25. the sale and purchase, lease and management of real estate properties;
26. the management of funds and powers to sign;
27. lending transactions backed by pledges on movable properties;
28. the organisation of and calls for tenders for contracts;
29. management, procurement and custody of gold that is owned;
30. deposit and management of deposits of gold belonging to third parties;
31. business in financial gold: the management of gold accounts – current accounts in XAU currency; the management of savings schemes in gold (investment programme involving the payment into current accounts in financial gold of constant amounts at regular intervals);
32. management of operations to purchase and sell gold with customers or partner banks;
33. processing, approval and management of loans of gold for its use including with a forward put option.

The activities identified as sensitive for the purposes of Decree 231 in UBI Banca with regard to crimes of terrorism and subversion of democratic law.

An analysis of the corporate processes of UBI Banca identified areas in which the types of crimes mentioned in article 25-*quater* of Decree 231 may theoretically be committed. A list of the activities considered “sensitive” or at risk with regard to crimes of terrorism and subversion of democratic law is given below, as examples but not limited to these, as follows:

1. the authorisation and provision of banking, financial and/or investment services;
2. the authorisation and provision of insurance services;
3. the management of investments other than banking and financial services (e.g. the acquisition of companies or stakes in companies, strategic agreements, other extraordinary finance transactions);
4. the negotiation, signing and performance of agency, intermediation, consultancy, financial advisor and brokerage contracts (selection, creation and regulation of relations, setting fees, management and termination of relations);
5. management of approval procedures, disbursement activities and the relative administrative formalities relating to the grant of loans and/or guarantees, inclusive of those which benefit from government subsidies and/or guarantees;
6. the implementation and/or promotion and management of sponsorships and commercial or humanitarian and charitable initiatives;
7. negotiation (by means of private negotiations or the organisation of public tenders) and management of relationships with consultants or suppliers of goods and/or services (management of the procurement process);
8. back-to-back transactions and correspondence relations with foreign banks;
9. the selection of commercial and financial partners and management of the relative relations;
10. selection and training activities for the proper application of the provisions of Legislative Decree No. 231/2007;
11. the administration of company servers or websites;

12. selection, appointment and management of personnel, including personnel belonging to protected groups or for whom concessions are granted for employing them;
13. the sale and purchase, lease and management of real estate properties;
14. lending transactions backed by pledges on movable properties;
15. the organisation of and calls for tenders for contracts;
16. business in financial gold: the management of gold accounts – current accounts in XAU currency; the management of savings schemes in gold (investment programme involving the payment into current accounts in financial gold of constant amounts at regular intervals);
17. management, procurement and custody of gold that is owned;
18. deposit and management of deposits of gold belonging to third parties;
19. management of operations to purchase and sell gold with customers or partner banks;
20. processing, approval and management of loans of gold for its use including with a forward put option;
21. the management of requests from investigative authorities (*carabinieri*, state police, financial police).

The activities identified as sensitive for the purposes of Decree 231 in UBI Banca with regard to crimes against the person of individuals.

An analysis of the corporate processes of UBI Banca identified areas in which the types of crimes mentioned in article 25-*quinquies* of Decree 231 may theoretically be committed. A list of the activities considered “sensitive” or at risk with regard to crimes against persons is given below, as examples but not limited to these, as follows:

1. management of approval procedures, disbursement activities and the relative administrative formalities relating to the grant of loans and/or guarantees, inclusive of those which benefit from government subsidies and/or guarantees;
2. activities which involve direct or indirect use of labour (e.g. awarding contracts, for cleaning, etc.);
3. the implementation, promotion and management of humanitarian and charitable initiatives;
4. the administration of company servers or websites;
5. the organisation and promotion of travel (e.g. vacation prizes) for employees or commercial partners (e.g. agents, account managers, etc.);
6. activities which involve the use of services provided by specialist agencies or tour operators.

The activities identified as sensitive for the purposes of Decree 231 in UBI Banca with regard to the crime of market rigging and the crimes (and corporate offences) of abuse of insider information and market manipulation.

Analysis of the corporate processes of UBI Banca identified the areas of the activities in which the crime of market rigging, the crimes mentioned in article 25 *sexies* of Decree 231 and the corporate offences referred to in Art. 187-*quinquies* of Legislative Decree No. 58/1998 may theoretically be committed. The activities identified as sensitive or at risk with regard to the crime of market rigging and the crimes (and corporate offences) of abuse of insider information and market manipulation are listed below, as examples but not limited to these, as follows:

1. the issue of information and more generally important information relating to the Bank through the media (e.g. press releases, website postings etc.), disclosures to markets and relations with financial analysts and rating agencies;
2. transactions involving financial instruments;
3. the management of insider information relating to the Bank or to third parties.

The activities identified as sensitive for the purposes of Decree 231 in UBI Banca with regard to transnational crimes.

An analysis of the corporate processes of UBI Banca identified the areas of activity in which the types of crimes mentioned in Law No. 146/2006 may theoretically be committed. A list of the activities considered “sensitive” or at risk identified with regard to transnational crimes is given below, as examples but not limited to these, as follows:

1. the authorisation and provision of banking, financial and/or investment services;
2. the authorisation and provision of insurance services;
3. the management of investments other than banking and financial services (e.g. the acquisition of companies or stakes in companies, strategic agreements, other extraordinary finance transactions);
4. the negotiation, signing and performance of agency, intermediation, consultancy, financial advisor and brokerage contracts (selection, creation and regulation of relations, setting fees, management and termination of relations);
5. management of approval procedures, disbursement activities and the relative administrative formalities relating to the grant of financial concessions and/or guarantees, inclusive of those which benefit from government subsidies and/or guarantees;
6. the appointment of members of the governing bodies of foreign companies in the Group;
7. the management of relations with members of governing bodies, employees or third parties involved in court proceedings;
8. the management of requests from investigative authorities (*carabinieri*, state police, financial police);
9. the management of activities designed to allow a person to physically enter a country;
10. the sale and purchase, lease and management of real estate properties;
11. the implementation and/or promotion and management of sponsorships and commercial or humanitarian and charitable initiatives;
12. assistance, consultancy or other forms of co-operation in the establishment, administration and management of trusts in relation to transnational activities;
13. negotiation (by means of private negotiations or the organisation of public tenders) and management of relationships with consultants or suppliers of goods and/or services (management of the procurement process);
14. the selection of commercial and financial partners and management of the relative relations in relation to transnational activities.
15. lending transactions backed by pledges on movable properties;
16. the organisation of and calls for tenders for contracts;
17. the management of banking, investment and insurance services to the benefit of a trust;
18. business in financial gold: the management of gold accounts – current accounts in XAU currency; the management of savings schemes in gold (investment programme involving the payment into current accounts in financial gold of constant amounts at regular intervals);
19. management, procurement and custody of gold that is owned;
20. deposit and management of deposits of gold belonging to third parties;
21. management of operations to purchase and sell gold with customers or partner banks;
22. processing, approval and management of loans of gold for its use including with a forward put option.

The activities identified as sensitive for the purposes of Decree 231 in UBI Banca with regard to crimes concerning health and safety at the workplace.

An analysis of the corporate processes of UBI Banca identified areas in which the types of crimes mentioned in article 25-septies of Decree 231 may theoretically be committed. Activities identified

as sensitive or at risk for crimes concerning health and safety at the workplace are listed, as examples but not limited to these, below:

1. the planning and organisation of roles and activities connected with health, safety and hygiene at the workplace;
2. the delegation of responsibilities to functions with regard to health, safety and hygiene at the workplace;
3. the identification, assessment and management of risks with regard to health, safety and hygiene at the workplace;
4. robbery and/or external violence risk management;
5. activity to inform personnel on matters concerning health, safety and hygiene at the workplace;
6. training activity with regard to health, safety and hygiene at the workplace;
7. relations with suppliers with regard to activities connected with health, safety and hygiene at the workplace;
8. the management of corporate assets with regard to activities connected with health, safety and hygiene at the workplace;
9. controls and corrective action with regard to activities connected with health, safety and hygiene at the workplace.

The activities identified as sensitive for the purposes of Decree 231 in UBI Banca with regard to crimes consisting of the receipt, laundering, use of money, goods or benefits of illicit origin and “self-laundering”.

An analysis of the corporate processes of UBI Banca identified areas in which the types of crimes mentioned in article 25-*octies* of Decree 231 may theoretically be committed. Activities identified as sensitive or at risk with regard to crimes consisting of the receipt, laundering and use of money, goods or benefits of illicit origin are listed below, as examples but not limited to these, as follows:

1. the authorisation and provision of banking, financial and/or investment services;
2. the authorisation and provision of insurance services;
3. the management of investments other than banking and financial services (e.g. acquisitions of equity investments or companies, strategic agreements, other extraordinary finance transactions);
4. the negotiation, signing and performance of agency, intermediation, financial advisor and brokerage contracts (selection, creation and regulation of relations, setting fees, management and termination of relations);
5. management of approval procedures, disbursement activities and the relative administrative formalities relating to the grant of loans and/or guarantees, inclusive of those which benefit from government subsidies and/or guarantees;
6. the implementation and/or promotion and management of sponsorships and commercial or humanitarian and charitable initiatives;
7. negotiation (by means of private negotiations or the organisation of public tenders) and management of relationships with consultants or suppliers of goods and/or services (management of the procurement process);
8. back-to-back transactions and correspondence relations with foreign banks;
9. assistance, consultancy or other forms of co-operation in the establishment, administration and management of trusts;
10. the selection of commercial and financial partners and management of the relative relations;
11. selection and training activities for the proper application of the provisions of Legislative Decree No. 231/2007;
12. the administration of company servers or websites;

13. selection, appointment and management of personnel, including personnel belonging to protected groups or for whom concessions are granted for employing them;
14. the sale and purchase, lease and management of real estate properties;
15. liquidity and intragroup treasury management;
16. the management of action taken to hedge risks resulting from business on own behalf and with the customers, including through the use of insurance policies;
17. price setting, management and adjustment for a service, product, relationship or transaction, including through wholesale actions and operations;
18. the management of financial operations and transactions with Italian and foreign institutional clients;
19. the management of intragroup financial operations and transactions;
20. activities to support the process of lodging banking assets eligible as collateral as part of Bank of Italy procedures;
21. all the administrative activities employed for the accurate determination of customer and bank tax affairs;
22. the management of administrative and back-office activities relating to deposit operations and other banking services (withdrawals, paying in, suspense accounts, foreign exchange and currency trading, etc.);
23. negotiation (by means of private negotiations or public tenders) and management of relationships with external counterparty customers relating to “income accounting cycle” processes;
24. administrative management of “income and expense accounting cycle” processes (invoicing, payments, receipts, etc.);
25. preparation of financial reports in compliance with obligations introduced by Law No. 262/2005 concerning company accounting documents;
26. management of relations with the tax authorities;
27. lending transactions backed by pledges on movable properties;
28. the organisation of and calls for tenders for contracts;
29. the management of banking, investment and insurance services to the benefit of a trust;
30. business in financial gold: the management of gold accounts – current accounts in XAU currency; the management of savings schemes in gold (investment programme involving the payment into current accounts in financial gold of constant amounts at regular intervals);
31. management, procurement and custody of gold that is owned;
32. deposit and management of deposits of gold belonging to third parties;
33. management of operations to purchase and sell gold with customers or partner banks;
34. processing, approval and management of loans of gold for its use including with a forward put option.

The activities identified as sensitive for the purposes of Decree 231 in UBI Banca with regard to computer crimes and the illicit processing of data.

An analysis of the corporate processes of UBI Banca identified an area in which the types of crimes mentioned in article 24-bis of Decree 231 may theoretically be committed. A list of the activities considered “sensitive” or at risk with regard to computer crimes and the illicit processing of data is given below, as examples but not limited to these, as follows:

1. the definition of rules to be adopted with regard to the safety of computer and electronic systems;
2. the management of access to computer systems by internal and external users, of user profiles and authentication processes;

3. the management of the security of legally valid electronic documents and the protection of networks and communications;
4. the management of physical and environmental security (including the security of equipment, wiring, network devices, information etc.) and of asset (tangible and intangible) inventory activities;
5. the acquisition and management of equipment, system devices (including detection devices) or software programmes (including the development of them and installation and maintenance services for them);
6. the monitoring and periodic verification of IT systems and the management of incidents and IT security problems;
7. the management of infrastructural aspects of on-line transactions.

The activities identified as sensitive for the purposes of Decree 231 in UBI Banca with regard to organised crime.

An analysis of the corporate processes of UBI Banca identified an area in which the types of crimes mentioned in article 24-ter of Decree 231 may theoretically be committed. A list of the activities considered “sensitive” or at risk with regard to organised crime is given below, as examples but not limited to these, as follows:

1. the authorisation and provision of banking, financial and/or investment services;
2. the authorisation and provision of insurance services;
3. the management of investments other than banking and financial services (e.g. acquisitions of equity investments or companies, strategic agreements, other extraordinary finance transactions);
4. the negotiation, signing and performance of agency, intermediation, financial advisor and brokerage contracts (selection, creation and regulation of relations, setting fees, management and termination of relations);
5. management of approval procedures, disbursement activities and the relative administrative formalities relating to the grant of loans including with concessions and/or guarantees, inclusive of those which benefit from government subsidies and/or guarantees;
6. the management of activities designed to allow a person to physically enter a country;
7. the sale and purchase, lease and management of real estate properties;
8. the implementation and/or promotion and management of sponsorships and commercial or humanitarian and charitable initiatives;
9. negotiation (by means of private negotiations or the organisation of public tenders) and management of relationships with consultants or suppliers of goods and/or services (management of the procurement process);
10. the selection of commercial and financial partners and management of the relative relations;
11. lending transactions backed by pledges on movable properties;
12. the organisation of and calls for tenders for contracts;
13. business in financial gold: the management of gold accounts – current accounts in XAU currency; the management of savings schemes in gold (investment programme involving the payment into current accounts in financial gold of constant amounts at regular intervals);
14. management, procurement and custody of gold that is owned;
15. deposit and management of deposits of gold belonging to third parties;
16. management of operations to purchase and sell gold with customers or partner banks;
17. processing, approval and management of loans of gold for its use including with a forward put option.

The activities identified as sensitive for the purposes of Decree 231 in UBI Banca with regard to crimes against industry and commerce.

An analysis of the corporate processes of UBI Banca identified an area in which the types of crimes mentioned in article 25-bis.1 of Decree 231 may theoretically be committed. A list of the activities considered “sensitive” or at risk with regard to crimes against industry and commerce is given below, as examples but not limited to these, as follows:

1. participation in tenders;
2. the organisation of tenders;
3. the management of relations with appointed parties or the direct performance of the following activities:
 - a) the sale of goods or services on the market;
 - b) the sale or marketing of foodstuff substances or products;
 - c) the sale or distribution of intellectual property or industrial products;
 - d) the introduction into the country for distribution of objects or other goods.
4. management, procurement and custody of gold that is owned;
5. deposit and management of deposits of gold belonging to third parties;
6. management of operations to purchase and sell gold with customers or partner banks.

The activities identified as sensitive for the purposes of Decree 231 in UBI Banca with regard to the violation of copyright.

An analysis of the corporate processes of UBI Banca identified areas in which the types of crimes mentioned in article 25-novies of Decree 231 may theoretically be committed.

The following activities:

- a) possession for any reason;
- b) importation
- c) distribution in any manner;
- d) reproduction or duplication;
- e) use for any reason;
- f) production;
- g) modification of the contents;

are considered as sensitive or at risk with regard to the violation of copyright where the activity relates, as examples but not limited to these, to the following:

- i) software programmes for computers;
- ii) means designed to violate barriers placed to protect software programmes;
- iii) the contents of databases;
- iv) media containing sound or video recordings of musical, cinematographic or audiovisual works or similar or sequences of images in movement;
- v) works or parts of literary, dramatic, scientific or didactic, musical or dramatic-musical or multimedia works even if they form part of collective or composite works of databases;
- vi) encrypted services;
- vii) special decoding devices or elements or the decoding of audiovisual transmissions performed by radio, satellite or cable in both analogical and digital form where access is subject to conditions;
- viii) equipment, products or components or services for which the primary purpose or commercial use is to penetrate effective technological protection measures;
- ix) other intellectual property or parts of it, or other material protected for copyright purposes, including property held in electronic form.

The activities identified as sensitive for the purposes of Decree 231 in UBI Banca with regard to environmental crimes.

An analysis of the corporate processes of UBI Banca identified areas in which the types of crimes mentioned in article 25- *undecies* of Legislative Decree No. 231/2001 may theoretically be committed. A list of the activities considered “sensitive” or at risk identified with regard to environmental crimes is given below, as examples but not limited to these, as follows:

1. waste disposal;
2. selection of suppliers and management of the relative relationships;
3. use and operation of heating and cooling systems.

The activities identified as sensitive for the purposes of Decree 231 in UBI Banca with regard to the employment of citizens of third party countries whose stay documents are irregular.

An analysis of the corporate processes of UBI Banca identified areas in which the types of crimes mentioned in article 25-*duodecies* of Legislative Decree No. 231/2001 may theoretically be committed. A list of the activities considered “sensitive” or at risk identified is given below, as examples but not limited to these, as follows:

1. selection, appointment and management of personnel, including personnel belonging to protected groups or for whom concessions are granted for employing them;
2. activities which involve direct or indirect use of labour (e.g. awarding contracts, for cleaning, etc.);
3. relations with agents, financial advisors and brokers (selection, creation and management of work relations);

The system of controls.

The controls designed to prevent the risk of crimes (and corporate offences) being committed that are relevant for the purposes of the corporate liability of entities, together with the provisions of the Code of Ethics, operate on two levels:

- **general protocols for activities**, which are always present in sensitive activities considered by the 231 Model;
- **general control principles** which contain specific rules designed to regulate particular aspects of sensitive activities.

The protocols contain provisions which are directly applicable and also others which are implemented through existing regulations (e.g. company regulations, procedures, circulars, etc.).

General protocols for the control of activities are as follows:

- a) **segregation of activities**: the performance of sensitive activities occurs by compliance with the principle of the segregation of activities between the person controlling and the person authorising;
- b) **rules**: the Bank adopts and applies organisational measures designed to furnish at least general principles to regulate sensitive activities in compliance with the provisions of the 231 Model;
- c) **powers to sign and powers to authorise**: the exercise of internal powers to sign and powers to authorise is performed on the basis of official rules introduced for that purpose;
- d) **traceability**: the persons and functions concerned and/or the IT systems used ensure the identification and traceability of the sources, information basis and controls performed which

support corporate decision-making and decision implementation and the manner of managing financial resources;

- e) **reports:** in cases where a senior officer of the Bank receives requests – or even learns of them through third parties – to carry out activities in violation of procedural rules provided for and referred to in the 231 Model, that person must immediately inform their hierarchical superior and the Chief Audit Executive of UBI Banca.

The general control principles are given in detail in the 15 sections – each one dedicated to a type of crime (and corporate offence) relevant for the purposes of the corporate liability of entities, which the Bank has decided to consider because of the nature of its business – which constitute the special parts of the Document Describing the Model.

The structure of each chapter is based on the association of the type of crime (described in section 1) with the sensitive activities identified by the Bank in relation to that type of crime (listed in section 2) and with the specific general control principles (section 3).

The general protocols and the general control principles were formulated with reference to the Italian Banking Association Guidelines, to the Confindustria Guidelines (confederation of industry), to those published to-date by the main business associations and to international best practices. They were subsequently adopted by the Bank with appropriate adaptations for its own governance model and organisational model.

In compliance with the specific provisions of the Italian Banking Association Guidelines, the risk assessment of crimes occurring and the formulation of regulations designed to prevent them were performed with consideration taken of the particular nature of the banking industry. They were based on the consequent assumption that generally the risk of occurrence for some types of offence in the Bank is the same as for that of any other type of entity (“general crimes”), but that for other types of crime there is a higher risk of occurrence in the Bank because of the nature of the business carried on by the Bank (“specific crimes”).

Again according to the guidelines just mentioned, for some types of crime (such as those relating to the receipt, laundering and use of money, goods or benefits of illicit origin), this distinction is of less importance because it is held that for the reasons specifically indicated, the crimes in question can be considered as both specific and general crimes with regard to banks.

As specifically concerns general crimes as previously defined, the system for the management of financial resources is not only governed by the regulations to implement the principles of “traceability” and “segregation” (the latter relating to the separation of duties and the opposition of functions) but also by the delegation of powers which is organised by the Bank in compliance with the regulations for “powers to sign and powers to authorise” which sets different levels of approval for spending by different parties and different procedures for signing on behalf of the Bank in the authorisation of financial transactions.

The specific general control principles for crimes regarding health and safety at the workplace have been formulated in compliance with Art. 30 of paragraph 5 of Legislative Decree No. 81/2008, by making reference to UNI-INAIL guidelines for the creation of a system to manage occupational health and safety.

The general control principles on computer crimes and the illicit processing of data have been formulated on the basis of the following:

- the ISO 27001 standard, which sets the requirements to be satisfied for an adequate information security management system (ISMS) for the proper management of sensitive corporate data;
- the COBIT framework, which represents the accepted standard for information and communication technology (ICT) management;
- the internationally recognised SAS 70 audit standard for security controls of service providers, which involve controls of networks, IT environments and the relative processes.

Where activities that are sensitive for the purposes of computer crimes and the illicit processing of data to which they are associated are outsourced and performed by other Group companies or by external providers, these specific general control principles may be incorporated in the service contracts for the performance of the activities.

Finally, in cases where a sensitive activity identified by the Bank is fully or partly performed by third parties in the name of and/or on behalf of the Bank, the following protocols shall apply in place of and/or to complete the specific general control principles in place for single sensitive activities:

- **contracts:** a specific contract is stipulated for every sensitive activity which is fully or partly outsourced, which regulates the performance of the sensitive activity and defines the service level (service level agreement) in a detailed and thorough manner, which clearly states the activities for which the Bank is responsible and those for which the outsourcer is responsible and it regulates the procedures by which, in compliance with the Model, the sensitive activities must be performed by the outsourcer;
- **contact:** for every activity which is fully or partially outsourced, a person or function is identified which is responsible for compliance with the provisions contained in the service level agreement in order to oversee the responsibilities of the Bank with regard to the externally outsourced activities;
- **special clauses:** special references to the regulations relating to the Model shall be contained in service contracts stipulated with third parties for the performance of sensitive activities and explicit termination clauses are inserted designed to penalise behaviour by third parties which violates the provisions of the Model;
- **controls:** in services contracts, third parties to whom the management of activities has been fully or partially outsourced, agree to take appropriate measures to prevent the commission of crimes and corporate offences relevant for the purposes of the corporate liability pursuant to Legislative Decree No. 231/2001 which could be ascribed to the Bank.