



ORGANIZATION, MANAGEMENT AND CONTROL MODEL

Under the terms of article 6, paragraph 3, of Legislative Decree no. 231 of 8 June 2001,
“Governing the administrative responsibility of corporate bodies, companies and associations including
those without legal personality, in compliance with article 11 of Law no. 300 of 29 September 2000”

Model approved by Board of Directors' resolution of 15 July 2009

A Foreword – the activity of COIMA s.r.l	4
1. The Legislative Decree	5
1.1 Administrative responsibility of entities	5
1.1.1 The fundamental principles of the Decree and related law	5
1.1.2 Sanctions	5
1.1.3 Types of offence	5
1.1.4 Public administration, public officials and individuals entrusted with a public service	6
1.1.5 Crimes against the public administration	7
1.1.6 Manslaughter and serious/very serious injury through negligence committed in breach of the occupational accident prevention and health and safety regulations	8
1.1.7 Receipt, laundering and use of money, assets or funds of criminal origin	8
1.1.8 Corporate offences	10
1.1.9 Market Abuses	11
1.1.10 Counterfeiting coinage, legal tender or revenue stamps	11
1.1.11 Activities intended to further to terrorism or subversion of the democratic order	11
1.1.12 Crimes against individuals and offences against the person	11
1.1.13 Transnational crime	12
1.1.14 Crimes committed overseas	12
1.1.15 Computer crime and the unlawful processing of data	12
1.1.16 Other crimes	13
1.2. Adoption of the Organization, Management and Control Model	14
1.2.1 Use of the Model as exemption in the event of an offence	15
1.2.2 COIMA and adoption of the Model: introduction	15
2. Adoption of the Model	16
2.1. Goals and adoption of the Model	16
2.1.1 Aims of the Model and its cardinal points	16
2.1.2 Approval of the Model	17
2.1.3 Amendments and revision of the Model	17
2.2 Addressees of the Model	17
3. Areas of risk	17
3.1 Crimes against the Public Administration	18
3.2 Corporate offences	19
3.3 Manslaughter and serious/very serious injury through negligence committed in breach of the occupational accident prevention and health and safety regulations	20
3.4 Computer crime	21
3.5 Other types of crime	21
3.6 Additional areas of risk	21
4. Procedures and principles of control	22
4.1 Crimes against the Public Administration	22
4.1.1 General codes of practice prescribed for the at risk areas of activity	22
4.1.2 Specific procedures for sensitive areas	23
4.2 Corporate offences	27
4.2.1 General codes of practice prescribed for the at risk areas of activity	27
4.2.2 Specific procedures for sensitive areas	28
4.2.3 Specific procedures for sensitive areas – corruption between private parties	29
4.3 Manslaughter and serious/very serious injury through negligence committed in breach of the occupational accident prevention and health and safety regulations	31
4.3.1 General principles of conduct prescribed in the area of activities at risk	31
4.3.2 Specific procedures for sensitive areas	32



4.4 Computer crime.....	34
4.4.1 General principles of conduct prescribed in the areas of activities at risk.....	34
4.4.2 Specific procedures for sensitive areas.....	35
5. Corporate Governance.....	35
5.1 General principles	35
5.2 The system of delegated powers and proxies	37
6. Supervisory Body.....	39
6.1 Identification of, appointment to and requirements for the Supervisory Body	39
6.2 Functions and powers of the Supervisory Body.....	40
7. Information flows.....	42
7.1 Reporting by the Supervisory Body to other Corporate Bodies	42
7.2 Reporting to the Supervisory Body: general prescriptions and mandatory specific prescriptions	42
7.3 Reporting by Company Members or third parties	43
7.4 Collection and storage of the information	43
8. Selection and training	44
8.1 Employees	44
8.2 External Contractors and Partners.....	44
9. Disciplinary system.....	45
9.1 General principles	45
9.2 Breach of the Model	45
9.3 Measures against Employees.....	45
9.4 Measures against Directors	46
9.5 Measures against Senior Officials.....	47
9.6 Measures against Contractors, Consultants and other third parties	47



A Foreword – the activity of COIMA s.r.l.

The purpose of the company COIMA S.r.l. (hereinafter “COIMA” and/or “Company”) is to:

build, redevelop, purchase, sell or exchange civil, industrial, residential, commercial, community, corporate or tourism buildings and infrastructure;

- renovate properties and carry out urban regeneration, landscaping, highways and monuments, either on its own behalf or on private or public commission, or acting as general contractor, in Italy and abroad;
- provide property and facility management for public and private entities; provide comprehensive administration, technical, accounting and data processing services in the management and valorization of the properties; provide auxiliary services for the operation of the properties, including maintenance work;
- organize and manage shopping centres, malls and integrated multipurpose centres, including administrative duties as well as marketing, commercial and executive services;
- supervise and coordinate the whole range of activities in the development of real estate assets;
- as foreseen by the articles of association, COIMA may also carry out any industrial, commercial or property operations seen as necessary or useful to achieving the company's purpose including (providing these activities are not conducted directly with the public and are strictly related with the achievement of the company's purpose):
 - purchase and sell shareholdings and stakes in companies and entities with purposes similar or in some way connected to its own;
 - give sureties and in general real or personal guarantees in favour of third parties.

COIMA specifically operates actively in the property development sector, providing due diligence and acting as project manager, construction manager, property & facility manager and auctions manager for a wide range of third party investors.

COIMA therefore:

- carries out activities related to the realization of new buildings, handling the engineering, design, development, construction and supervision;
- identifies investment opportunities, realizing new properties as part of development initiatives and the strategic management of the acquired portfolios for the purposes of their valorization, organization, maintenance and management;
- identifies, proposes and participates in investment opportunities in the property market, providing all the functions necessary to the structuring of the deal and the subsequent management and disposal of the properties purchased;
- acts as project manager (purchasing, planning and realization, reporting, administration, rental and sale) for the managing and realization of development and urban redevelopment projects.

The above activities may either be performed directly by the company's own personnel or by third party subcontractors engaged by COIMA to carry out various stages of the work.

1. The Legislative Decree

1.1 Administrative responsibility of entities

Legislative Decree no. 231 of 8 June 2001 “Governing the administrative responsibility of corporate bodies, companies and associations including those without legal personality, in compliance with article 11 of Law no. 300 of 29 September 2000” (hereinafter, the “**Decree**”), which came into force on 4 July 2001, introduced into Italian law criminal liability for entities (corporations, companies and associations including those without legal personality), in addition to that for the natural persons who represent them and who are materially responsible for committing the offences.

The law states that entities may be held responsible and therefore sanctioned, for offences committed or attempted in the interest, or to the benefit, of the entity itself by its directors or employees.

1.1.1 The fundamental principles of the Decree and related law

The Decree set out to bring Italian law on corporate liability into line with the international treaties to which Italy was a signatory, such as:

- the *European Community Brussels Convention of 26 July 1995* on the protection of financial interests;
- the *Convention of 26 May 1997*, again signed in Brussels, on the fight against corruption of EU or Member State officials; and
- the *OECD Convention of 17 December 1997* on combating bribery of foreign public officials in international business transactions.

The Decree introduced into Italian law a regime of administrative responsibility (largely concerning criminal liability) of entities (understood as companies, associations, consortiums, etc., hereinafter “Entities”) for a range of offences, in the interest, or to the benefit, of the Entities themselves, by:

- natural persons with representative, administrative or executive positions within the Entities themselves or by one of the organizational units with financial and functional autonomy;
- natural persons exercising de facto management control within the Entities;
- natural persons under the direction or supervision of the above individuals.

This liability is additional to the (criminal) liability of the individual who materially committed the offence.

1.1.2 Sanctions

The sanctions¹ against the Entity foreseen for the commission or attempted commission of the above offences, are:

- fines (up to 1.5 million euros);
- disqualifications, such as a ban on exercising a certain activity, the suspension or revocation of licenses or permits, a ban on signing contracts with the Public Administration, the exclusion or revocation of loans and funding, a ban on advertising of goods and services;
- confiscation (and pre-trial preliminary seizure) of any profits which the Entity might have obtained from the offence, or the equivalent²;
- publication of the sentence (in the event of a disqualification³).

1.1.3 Types of offence

The types of offence covered by the Decree and its subsequent amendments and additions fall into the following categories:

¹ Article 9 and successive articles, Title I, Section II “General Sanctions” of the Decree.

² Article 6, paragraph 5.

³ Article 18, Section II cited

- offences against the Public Administration⁴;
- corporate offences⁵;
- market abuse⁶;
- manslaughter and serious/very serious injury through negligence committed in breach of the occupational accident prevention and health and safety regulations⁷;
- receipt, laundering and use of money, assets or funds of criminal origin⁸;
- crimes against public trust⁹ counterfeiting coinage, legal tender or revenue stamps;
- offences relating to terrorism and subversion of the democratic order, and the financing of the such ends¹⁰;
- offences against the person, such as the exploitation of child prostitution, child pornography also via the Internet, the trafficking of people reduced to and held in slavery¹¹ and, among offences against the person, female genital mutilation¹²;
- transnational crimes;
- computer crime and the unlawful processing of data;
- organized crime offences;
- crimes against trade and industry;
- copyright offences;
- inducing someone to make a false statement or commit perjury
- environmental crime;
- employment of foreign citizens without a legal stay permit for Italy.

1.1.4 Public administration, public officials and individuals entrusted with a public service

Public Administration

The Decree defines the Public Administration as all subjects, private and public, who perform a “public function” or a “public service”.

Public function and public official

By public function is meant any activity governed by public law pertaining to:

- *legislative functions* (state, regional, provincial government, etc.),
- *administrative functions* (members of state and territorial administrations, forces of law and order, members of supranational administrations such as the EU, members of authorities, antitrust bodies, chambers of commerce, planning commissions, public works inspectors, Italian Naval Register experts, etc.); and *judicial functions* (judges, justice officials, individuals accessory to the justice system such as official receivers or liquidators, etc.).

Public officials exercise their function through authoritative or certification powers. Note that:

- authoritative power is that which allows the Public Administration to achieve its ends by effective command, to which private individuals are subject. Through it is expressed so-called power of sovereignty, including the power to coerce (arrest, search, etc.) and report violations of the law (inspection of breaches etc.), and the powers of hierarchical supremacy in public office;
- certification power is the certifier's ability to attest a fact in such a way that is proof against allegations of falsehood.

⁴ Articles 24 and 25, Title I, Section II of the Decree “Administrative responsibility for crimes foreseen by the criminal code”.

⁵ Article 25-ter, Section III cited.

⁶ Article 25-sexies.

⁷ Article 25-septies.

⁸ Article 25-opties.

⁹ Article 25-bis, Section III cited.

¹⁰ Article 25-quarter, Section III cited.

¹¹ Article 25-quinquies, Section III cited.

¹² Article 25-quarter.

Article 357 of the Criminal Code defines “public official” as one who “exercises a legislative, judicial or administrative public function”.

Public service and individuals entrusted with public service

Public service is understood to mean:

- the provision of goods and services of general interest and subject to the supervision of a public regulator;
- activities designed to guarantee the rights of the person to life, health, freedom, welfare and pension provision, education, freedom of speech etc., through a concession and/or agreement (e.g., public hospitals, health trusts, I.N.P.S., I.N.A.I.L., city councils, banks, post offices, customs, railways, motorways, municipal energy companies, airlines etc.).

public service is governed in the same way as the public function, but is characterized by a lack of the powers typical of the latter (authoritative and certification powers) and does not involve the performance of routine duties and purely menial work.

Article 358 of the Criminal Code defines a “person entrusted with a public service” as someone who “in any way performs a public service”.

1.1.5 Crimes against the public administration

The Decree lists a number of specific crimes against the public administration entailing the liability of Entities. These are:

- **embezzlement at the expense of the state or another public or community body**¹³: failure to allocate funds, subsidies or similar to the purposes for which they were intended;
- **improper receipt of funds, loans or other monies** by the state or another public or community body¹⁴ through the use of false documents or issuing false statements, or a failure to provide proper information;
- **aggravated fraud in order to obtain public monies**¹⁵: receipt of funds, loans or other monies by the state of another public or community body through various ploys or deceptions other than the use of false documents, false statements or failure to provide proper information;
- **aggravated fraud at the expense of the state or another public body**¹⁶: use of ploys and deceptions to profit unlawfully at the expense of the state or another public body;
- **computer fraud at the expense of the state or another public body**¹⁷: tampering with an IT or telemetric system, or unauthorized use of data, information or programmes in an IT system to profit unlawfully at the expense of the state or another public body.
- **extortion**¹⁸, where a public official or person entrusted with a public service abuses his/her position and power to force or induce an individual to give or promise money or other benefit;
- **bribing a public official to do something**¹⁹, where a public official or person entrusted with a public service receives (or agrees to receive) money or other benefit to perform a public act;
- **bribing a public official not to do something**²⁰, where a public official or person entrusted with a public service receives (or agrees to receive) money or other benefit for themselves or for someone else to delay a public act or perform a public act contrary to their duty;
- **corruption of judicial proceedings**²¹: in both the above cases of corruption, the case in which the person who receives (or agrees to receive) a benefit for him/herself or for another in order to favour or damage one side of a civil, administrative or criminal trial;
- **improper inducement to a give or promise a benefit**²²: where a public official or person entrusted with a public service abuses their position and powers to force or induce an individual to give or promise

¹³ Article 316-bis of the Criminal Code.

¹⁴ Article 316-ter of the Criminal Code.

¹⁵ Article 640-bis of the Criminal Code.

¹⁶ Article 640, paragraph 2, no. 1 of the Criminal Code.

¹⁷ Article 640-ter of the Criminal Code.

¹⁸ Article 317 of the Criminal Code.

¹⁹ Article 318 of the Criminal Code.

²⁰ Article 319 of the Criminal Code.

²¹ Article 319-ter of the Criminal Code.

money or other benefit to them or a third party; the criminal liability also extends to the person who gives or promises the money or other benefit;

- **incitement to corruption**²³: in both above cases of corruption, the case in which the public official does not accept, or the private individual refuses to give, the money or other benefit .
- **embezzlement, extortion, misappropriation, improper incitement** to give or promise a benefit, bribery and incitement to corrupt members of the International Criminal Court or European Union bodies and European Union and foreign member state officials²⁴: the hypothesis foreseen by the law is that any of the offences listed above are involve foreign officials.

1.1.6 Manslaughter and serious/very serious injury through negligence committed in breach of the occupational accident prevention and health and safety regulations

Law no. 123 of 3 August 2007, published in Official Journal no. 185 on 10 August 2007, which came into force on 25 August 2007, introduces into Legislative Decree no. 231/01 article 25 septies, subsequently amended by the Consolidated Law on Safety: the entity is also liable for:

- manslaughter (article 589 of the Criminal Code) and
- serious/very serious injury through negligence (article 590 of the Criminal Code),

where manslaughter is committed in breach of article 55, paragraph 2 of the Consolidated Law on Safety, or the offences in question are committed in breach of the occupational accident prevention and health and safety standards.

The relevant standards are contained in the Consolidated Law on Safety.

What is more, it should be specified that any breach of the employer's obligation to guarantee safety in the workplace (article 2087 of the Civil Code) - causing severe injury - automatically entails a judicial lawsuit against the company.

The justice system has established that a breach of the safety at work standards aggravates the crimes of manslaughter and serious/very serious injury through negligence, rendering article 25-septies of Legislative Decree no. 231/2001 applicable.

Serious/very serious injuries (article 583 of the Criminal Code) are injuries which cause:

- life-threatening illness or illness or incapacity to work normally for more than forty days;
- permanent impairment of one of the senses or a bodily organ; illness which is certainly or probably incurable; loss of one of the senses; loss of a limb, or mutilation rendering the limb unusable, or loss of the use of an organ or the ability to procreate, or permanent and severe impairment to speech; deformation or permanent disfigurement of the face.

It must be stressed that in these cases the crime is punishable on the basis of mere fault, unlike other predicate offences which must be committed deliberately and voluntarily.

The Entity must therefore to adopt an Organizational Model which incorporates the analysis of risks connected with the standards on health and safety in the workplace.

1.1.7 Receipt, laundering and use of money, assets or funds of criminal origin

Legislative Decree of 16 November 2007, which ratifies directive 2005/60/EC of 26 October 2005, and directive 2006/70/EC of 1 August 2006, introduces in the framework of Legislative Decree no. 231/01 the cases foreseen by articles 648 (receipt), 648-bis (money laundering) and -ter (use of money, assets or funds of criminal origin).

Note that where articles 648-bis and -ter already constituted liable offences for the corporation within the framework of transnational offences (Law no. 146/2006), the crime of receipt (article 648 of the Criminal Code), is included among the predicate offences for the first time.

²² Article 319-quarter of the Criminal Code.

²³Article 322 of the Criminal Code.

²⁴Article 322-bis of the Criminal Code.

These crimes share some **common characteristics but also some elements of differentiation**.

The law intends, where an offence is committed (so-called predicate offences), to prevent people other than those who committed it (“Except in cases of complicity...”) becoming interested in the events caused by the offence. The heart of the three alleged crimes, therefore, lies in the **activity subsequent** to the commission of the offence, activity which nevertheless involves an assault on the legal asset (the law is designed to prevent any economic gain from the proceeds of crime) and on the administration of justice (the assets of unlawful origin may be dispersed by criminal conduct to create obstacles to the authorities in the detection and repression of the predicate offences).

The differences between articles 648, 648-bis and 648-ter of the Criminal Code, instead, lie essentially in the conduct (material element) and the subjective element (generic or specific intent)²⁵.

Regarding the material element:

- **Receiving stolen goods:** offences include purchasing, receiving, concealing or involvement in purchasing, receiving or concealing money or goods proceeding from crime
- **Money laundering:** offences include replacing, transferring, or carrying out other operations so as to obstruct the identification of the criminal origins of money, assets or other benefits.
- **Use of money, assets or funds of criminal origin:** offences include using money, assets or benefits of criminal origin in business or financial activities.

Regarding the subjective element:

- **Receiving stolen goods:** behaviour intended to procure gain for oneself or for others (specific intent).
- **Money laundering:** this offence involves generic intent.
- **Use of money, assets or funds of criminal origin:** this offence involves generic intent.

Among these three types of crime in the context of corporate criminal law, money laundering certainly represents the most significant case and, therefore, the most important risk to be considered. In Italy the law on money laundering was introduced by Legislative Decree no. 59 of 21 March 1978 and converted into Law no. 191 of 18 May 1978, which introduced article 648-bis of the Criminal Code, recorded at the time as “recycling of money or goods originating from aggravated robbery, aggravated extortion or kidnapping with the intention of extortion”.

It therefore represents a **special type of receipt** of money originating from one of these offences.

With the reform of 1990 (article 23, Law no. 55 of 19 March 1990), the intent to profit disappeared (subjective element) and the definition of conduct was based on **obstructing the identification of the criminal origins of the assets**, the salient point of the current legislation.

It also added article 648-ter of the Criminal Code which punished the behaviour subsequent to and independent from the money laundering, i.e. the use of money originating from the above offences in business or financial activities. It therefore concerns behaviour subsequent to the commission of the predicate offence and the laundering of money or other proceeds of crime.

A later reform, Law no. 328/1993 ratifying the Convention of Strasbourg of 8 November 1990, retains the 1990 framework, but removes the **specific list** of predicate offences in favour of the generic criminal origin of the money.

The law, which is constantly evolving, foresees limitations to the use and transfer of cash, the obligation on financial intermediaries to identify and register clients and report suspicious transactions, as well as rules for the prevention of criminal behaviour (the “know your customer” rule and the quantitative analyses of transactions) which can also influence the content of the compliance model.

²⁵“Money laundering is not distinguished from the offence of receiving stolen goods under article 648 of the Criminal Code on the basis of the predicate offences; the difference should be sought in the structural aspects, such as the **subjective element**, which refers to the specific intent of profiting from the receipt and the generic intent of money laundering, and the **material element**, and in particular the intention to obstruct the identification of the origin of the assets, which is a characteristic feature of the conduct covered by article 648-bis of the Criminal Code.” (Criminal Court of Cassation, 12 April 2005, De Luca appeal).

1.1.8 Corporate offences

Within the framework of the reform of corporate law, Legislative Decree no. 61 of 11 April 2002²⁶, which came into force on 16 April 2002, introduced a new article 25-ter of the Decree, extending the system of administrative responsibility of Entities to so-called “corporate offences”.

Corporate offences are crimes which may be **committed directly** by the:

- Board of Directors
- Directors
- General Managers
- Auditors
- Official Receivers

and, by collusion, with the units responsible for the administrative/accounting and financial activities or implementation of the accounting information system.

The types of corporate offences considered are:

- **misleading corporate communications** (article 2621 of the Civil Code): in company communications required by law stating material facts which do not correspond to the truth or omit the required information on the company's business, equity or financial position;
- **company communications which mislead shareholders or creditors** (article 2622, paragraphs 1 and 2, of the Civil Code): in company communications required by law give material facts which do not correspond to the truth or omit the required information on the company's business, equity or financial position, where this causes damage to the shareholders or creditors;
- **improper repayment of contributions** (article 2626 of the Civil Code): repay shareholders their contributions or release them from the obligation of disclosure;
- **unlawful allocation of profits and reserves** (article 2627 of the Civil Code): allocate profits or reserves which may not be distributed by law;
- **unlawful transactions of shares or quotas of the company or parent company** (article 2628 of the Civil Code): purchase or subscribe shares, including those of the parent, resulting in harm to the share capital;
- **transactions prejudicial to the creditors** (article 2629 of the Civil Code): reduce the share capital, or realize mergers or spin-offs which cause harm to the creditors;
- **failure to disclose conflicts of interest** (article 2629-bis of the Civil Code): violation of the obligation to disclose a conflict of interest, with prejudice to the company or to third parties;
- **fictitious formation of capital** (article 2632 of the Civil Code): artificially increase the capital, subscribe shares reciprocally and overestimate contributions or equity in the event of a transformation;
- **improper distribution of corporate assets by the official receivers** (article 2633 of the Civil Code): distribute corporate assets before the payment of creditors or before the provision of the sums required to pay them;
- **obstructing control** (article 2625, paragraph 2, of the Civil Code): conceal documents in order to prevent control by shareholders or other corporate bodies;
- **unlawful influence on the Shareholders' Meeting** (article 2636 of the Civil Code): dissimulation or fraudulent activity designed to create fictitious majorities at the Shareholders' Meeting;
- **bribery of private individuals** (article 2635, paragraph 3 of the Civil Code): give or promise money or other benefits (as corrupter) to directors, general managers, persons charged with drawing up the financial statements, auditors and liquidators, who, following the giving or promise of money or other benefits, either to them or others, act or fail to act in breach of the obligations inherent to their office or the obligations of loyalty, thereby causing damage to the company (as the corrupted entity); under Legislative Decree no. 231/2001 liability regards the corrupter;
- **stock manipulation** (article 2637 of the Civil Code): disseminate false information or make fictitious transactions designed to alter the stock price of unlisted financial instruments;
- **obstruct the work of the supervisory authorities** (article 2638, paragraphs 1 and 2, of the Civil Code): make factually untrue statements designed to obstruct the work of the supervisor in its valuation of the

²⁶ Article 3

business, equity or financial situation or for the same purpose hide by fraudulent means facts which should be disclosed.

1.1.9 Market Abuse

Among corporate offences in the widest sense we should mention market abuse, governed by Law no. 62 of 18 April 2005:

- **abuse of inside information** (article 184 of Legislative Decree no. 58/1998), by anyone who, by virtue of their “privileged” position (member of the board of directors, management or a control body of the issuer, or a shareholder of the issuer) uses such information to operate on financial markets;
- **market manipulation** (article 185 Legislative Decree no. 58/1998) by anyone who disseminates false information or sets up artificial schemes designed to cause a sizable change in the stock price of the financial instruments.

1.1.10 Counterfeiting coinage, legal tender or revenue stamps

Law no. 409 of 23 November 2001 providing “Urgent provisions in view of the introduction of the Euro”, introduces within the framework of the Decree article 25-bis, which punishes “counterfeiting coinage, legal tender and revenue stamps” , the following other types of corporate crime:

- **forgery, spending and introduction in the state of counterfeit money, following prior agreement** (article 453 of the Criminal Code);
- **forgery of coinage** (article 454 of the Criminal Code);
- **counterfeiting of watermarked paper used to produce legal tender or revenue stamps** (article 460 of the Criminal Code)
- **manufacturing or possession of watermarks or tools used to forge coinage, revenue stamps or watermarked paper** (article 461 of the Criminal Code);
- **spending and introduction in the state of counterfeit money, without prior agreement** (article 455 of the Criminal Code);
- **spending of counterfeit money received in good faith** (article 457 of the Criminal Code);
- **use of counterfeit or forged revenue stamps received in good faith** (article 464, paragraph 2 of the Criminal Code);
- **forgery of revenue stamps, introduction in the state, purchase, possession or circulation of counterfeit revenue stamps** (article 459 of the Criminal Code);
- **use of counterfeit or forged revenue stamps** (article 464, paragraph 1 of the Criminal Code).

1.1.11 Activities intended to further to terrorism or subversion of the democratic order

Law no. 7 of 14 January 2003 ratified the International Convention for the Suppression of the Financing of Terrorism, signed in New York on 9 December 1999.

Unlike other types of corporate crime, there is no precise list of offences. Any crime committed to further terrorism or subversion of the democratic order entails corporate liability.

1.1.12 Crimes against individuals and offences against the person

The crimes in question are:

- **reducing people to or holding them in slavery or servitude** (article 600 of the Criminal Code): reducing people to or holding them in a state of continual subjection, forcing them to work by exploitation;
- **people trafficking** (article 601 of the Criminal Code): trading of slaves or people in similar conditions;
- **purchase and sale of slaves** (article 602 of the Criminal Code): any conduct which involves the transfer of slaves or people in similar conditions;

- **child prostitution** (article 600-bis, paragraph 1 and 2 of the Criminal Code): inducement, favouring or exploitation of child prostitution, or performing sexual acts with minors in exchange for money or other economic benefit;
- **child pornography** (article 600-ter, paragraphs 1, 2, 3 and 4 of the Criminal Code): exploitation of minors to realize pornographic films or material; trade in pornographic material produced by exploitation; distributing, divulging, publicizing pornographic material realized through the exploitation of minors, or disseminating information aimed at grooming or exploiting minors;
- **tourism based on the exploitation of child prostitution** (article 600-quinquies of the Criminal Code): organizing or marketing travel aimed at the enjoyment of child prostitution;
- **possessing child pornography** (article 600-quarter of the Criminal Code): obtaining or merely having available pornographic material realized through the exploitation of minors;
- **virtual pornography** (article 600 quater.1. of the Criminal Code): child pornography and possession of child pornography in which the material is represented by virtual images;
- **female genital mutilation** (article 583-bis of the Criminal Code) for non-medical reasons.

1.1.13 Transnational crime

Transnational offences, introduced by Law no. 146 of 16 March 2006, ratifying and executing the United Nations Convention and Protocols against Organized Crime, are those committed by criminal associations operating across several countries and comprise the following:

- **criminal conspiracy**: association by at least three people for the purposes of committing an unspecified series of offences;
- **mafia-type criminal conspiracy**: criminal conspiracy which uses the power of intimidation based on the associative bond, as well as the condition of subjection and code of silence connected with it;
- **criminal conspiracy to traffic contraband foreign tobacco products**: criminal conspiracy to introduce, sell, transport, purchase or possess foreign-made tobacco products in the territory of the state;
- **criminal conspiracy to traffic drugs**: criminal conspiracy to commit drug trafficking;
- **trafficking of migrants and illegal immigrants**: aiding and abetting illegal immigration and assisting illegal immigrants to stay in the country;
- **money laundering**: recycling or transfer of money, assets or funds of criminal origin, and activity intended to obstruct the detection of the proceeds of crime;
- **use of money, assets or funds of criminal origin**;
- **inducement to refuse to make a statement**: inducing persons required to make statements to the judicial authorities, to make false statements, or to make no statement, using threats, violence and offers of money;
- **aiding and abetting**: helping a person who has committed a crime to avoid investigation or evade the justice system.

1.1.14 Crimes committed overseas

The Decree also foresees liability for crimes committed abroad for offences named in the criminal code articles 7, 8, 9 and 10, providing they are not under investigation in the state in which the crime was committed.

1.1.15 Computer crime and the unlawful processing of data

Legislative Decree no. 48 of 4 April 2008, which ratifies and executes the Council of Europe Budapest Convention on Cybercrime, introduces within the framework of Legislative Decree no. 231/01 the following offences:

- **falsification of IT documents** (article 491-bis of the Criminal Code);
- **unauthorized access to an IT or telemetric system** (article 615-ter of the Criminal Code);

- **possession and illicit circulation of passwords to computing or telemetric systems** (article 615 quarter of the Criminal Code);
- **distribution of equipment, devices or computer programmes intended to damage or interrupt an IT or telemetric system** (article 615-quinquies of the Criminal Code);
- **interception, impediment or unlawful discontinuation of IT or telemetric communications** (article 617 quarter of the Criminal Code);
- **installation of equipment to intercept, prevent or interrupt IT or telemetric communications** (article 617-quinquies of the Criminal Code);
- **damage to IT information, data or programmes** (article 635-bis of the Criminal Code);
- **damage to IT information, data and programmes used by the state or another public body or public utility** (article 635-ter of the Criminal Code);
- **damage to IT or telemetric systems** (article 635-quater of the Criminal Code);
- **damage to IT or telemetric systems of public utility** (article 635-quinquies of the Criminal Code);
- **computer fraud by an entity charged with providing digital signature certification services** (640-quinquies of the Criminal Code).

1.1.16 Other crimes

Law no. 94 of 15 July 2009 “On matters of public safety”, which came into force on 8 August 2009, introduces into the Decree article 24-ter **On Organized Crime**, which extends the corporate liability of entities to the following offences:

- criminal conspiracy (article 416 of the Criminal Code)
- mafia-type criminal conspiracy (article 416-bis of the Criminal Code);
- mafia-type electoral fraud (article 416-ter of the Criminal Code);
- kidnapping for the purposes of robbery or extortion (article 630 of the Criminal Code);
- crimes committed under the conditions covered by article 416-bis, i.e. to facilitate mafia-type criminal offences;
- criminal conspiracy to traffic drugs or psychoactive substances (article 74 of the Decree of the President of the Republic no. 309 of 9 October 1990);
- illegal manufacture, introduction in the state, sale, trade, possession and carrying in a public place or a place open to the public of military or military-type firearms;
- or parts of them, explosives, banned firearms as well as common firearms apart from those described in article 2, paragraph 3, of Law no. 110 of 18 April 1975.

Law no. 99 of 23 July 2009 “Provisions on the growth and internationalization of companies, and energy-related matters”, which came into force on 15 August 2009, introduces in the Decree the following offences: crimes against trade and industry; copyright offences:

- disturbance to freedom of industry or trade (article 513 of the Criminal Code);
- unlawful competition with threat or violence (article 513-bis of the Criminal Code);
- fraud against national industries (article 514 of the Criminal Code);
- fraud in the exercise of commerce (article 515 of the Criminal Code);
- sale of non-genuine food substances as genuine (article 516 of the Criminal Code);
- sale of manufactured products with misleading labels (article 517 of the Criminal Code);
- manufacturing and trade of goods produced using stolen industrial property (article 517-ter of the Criminal Code);
- counterfeiting of geographical indications or controlled designations of origin for agri-food products (article 517-quarter of the Criminal Code);
- copyright offences (articles 171, paragraph 1, letter a-bis, and paragraph 3, 171-bis, 171-ter, 171-septies and 171-octies of Law no. 633 of 22 April 1941).

Law no. 116 of 3 August 2009 “Ratification and execution of the United Nations Convention against Corruption, adopted by the General Assembly of the U.N. on 31 October 2003 by resolution 58/4, signed by

the Italian State on 9 December 2003, as well as domestic amendments and adjustments to the criminal code and criminal procedure”, introduced within the framework of the Decree the crime of **inducing someone to make a false statement or commit perjury** (article 377-bis of the Criminal Code)

Legislative Decree no. 121 of 7 July 2011: “Enacting directive 2008/99/EC on the criminal protection of the environment, and directive 2009/123/EC amending directive 2005/35/EC on pollution by shipping and the introduction of sanctions for violations”, introduces among the offences covered by the Decree “**Environmental Crime**”, including:

- the killing, destruction, capture, hunting, possession of protected wild animals or plants (article 727-bis of the Criminal Code);
- the destruction or damage to habitat within a protected site (article 733-bis of the Criminal Code);
- trade in specimens of the species listed in annex A, appendix I, and annex C, part 1 of Regulation (EC) no. 338/97 (article 1, Law no. 150 of 7 February 1992);
- trade in specimens of the species listed in annex A, appendices I and III, and annex C, part 2 of Regulation (EC) no. 338/97 (article 2, Law no. 150 of 7 February 1992);
- ban on possession of specimens representing a public health or safety hazard (article 6, Law no. 150 of 7 February 1992);
- discharge of waste waters (article 137 Legislative Decree no. 152 of 3 April 2006);
- waste discharges on soil (article 103 Legislative Decree no. 152 of 3 April 2006);
- waste discharges into subsoil and underground water (article 104 Legislative Decree no. 152 of 3 April 2006);
- discharges into sewage networks (article 107 Legislative Decree no. 152 of 3 April 2006);
- discharge of hazardous substances (article 108 Legislative Decree no. 152 of 3 April 2006);
- handling of unauthorized wastes (article 256 and articles 208, 209, 210, 211, 212, 214, 215, 216 of Legislative Decree no. 152 of 3 April 2006);
- ban on abandonment of wastes (article 192 Legislative Decree no. 152 of 3 April 2006);
- ban on mixing hazardous wastes (article 187 Legislative Decree no. 152 of 3 April 2006);
- electrical and electronic refuse, sanitary refuse, disused vehicles and products containing asbestos (article 227 Legislative Decree no. 152 of 3 April 2006);
- decontamination of sites (article 257 Legislative Decree no. 152 of 3 April 2006);
- breach of obligations of disclosure, keeping registers and forms (article 258 Legislative Decree no. 152 of 3 April 2006);
- falsehood by a private individual in a public statement (article 483 of the Criminal Code);
- unlawful trafficking of wastes (article 259 Legislative Decree no. 152 of 3 April 2006);
- organized trafficking of illegal wastes (article 260 Legislative Decree no. 152 of 3 April 2006);
- forgery of certificates or authorizations by a public official (article 477 of the Criminal Code);
- forgery of certificates or authorizations by a private individual (article 482 of the Criminal Code);
- termination and reduction of use of harmful substances (article 3 Law no. 549 of 28 December 1993);
- malicious pollution by shipping (article 8 Legislative Decree no. 202 of 6 April 2007);
- negligent pollution by shipping (article 9 Legislative Decree no. 202 of 6 April 2007).

Legislative Decree no. 109/2012: “Enacting directive 2009/52/EC which introduces minimum sanctions and measures against those who employ citizens of foreign countries without a valid stay permit” introduces with article 25-duodecies of Legislative Decree no. 231/01 the offence pursuant to article 22 paragraph 12-bis of Legislative Decree no. 286/1998 (**employment of foreign citizens without a legal stay permit for Italy**).

1.2. Adoption of the Organization, Management and Control Model

The Decree²⁷ introduces a special waiver of liability if the Entity can demonstrate that:

²⁷ Article 6, paragraph 1.

- a) prior to the commission of an offence, it has adopted and effectively implemented via the governing body an Organization and Management Model designed to prevent such offences;
- b) it has set up an internal body, with independent powers of initiative and control, to monitor the workings and observance of the models, and ensure that it is kept up-to-date;
- c) the persons who committed the offence deceitfully circumvented the aforementioned organization and management models;
- d) the body described in point b) above did not fail in its duty of surveillance.

1.2.1 Use of the Model as exemption in the event of an offence

The Decree also states that, regarding the extent of the delegated powers and the risk of offences being committed, the Organization, Management and Control Models must²⁸:

- 1. identify all areas in which there is a risk that the offences covered by the Decree might be committed;
- 2. contain specific protocols for training and implementation of the entity's resolutions regarding the offences to be prevented;
- 3. foresee means of finding and employing sufficient financial resources to prevent the commission of such offences;
- 4. establish obligations to report to the body entrusted with monitoring the workings and observance of the Model;
- 5. create an internal disciplinary system to sanction any failures to observe the measures specified in the Model.

The Decree states that Organization, Management and Control Models meeting the above requirements be adopted through codes of practice (e.g., guidelines) drawn up by the trade associations, and communicated to the Ministry of Justice so that, in concert with the other competent ministries, it may (within 30 days) furnish observations on the fitness of the Models to prevent the said offences²⁹.

Finally the Decree foresees that, in the case of smaller Entities, supervisory control may be carried out directly by the governing body³⁰.

1.2.2 COIMA and adoption of the Model: introduction

In order to guarantee ever greater conditions of propriety and transparency in the conduct of its corporate affairs, COIMA has chosen to adopt an "Organizational, Management and Control Model" in line with the provisions of the decree (hereinafter "**Model**"), as described in detail in chapter 2 below.

The company believes that, above and beyond the requirements of the law, in adopting the Model, together with the Code of Ethics (Annex 1) it can ensure that all employees and everyone who works with it are fully aware of the correct and transparent practices to be adhered to in the fulfilment of their duties, in line with the ethical and social values which inspire COIMA in pursuit of its corporate goals, and as such prevent the commission of the offences described by the Decree.

In the preparation of this Model, COIMA analysed the various areas of risk bearing in mind the recommendations of the Decree and the Confindustria Guidelines.

In enacting the requirements of the Decree, the COIMA Board of Directors appointed Professional Governance Overview Srl., as supervisory body (hereinafter "**Supervisory Body**"), charged with overseeing the workings, effectiveness and observance of the Model, and ensuring that it is kept up-to-date.

²⁸ Article 6, paragraph 2.

²⁹ Article 6, paragraph 3.

³⁰ Article 6, paragraph 4.

2. Adoption of the Model

The company

COIMA is a limited liability company with the functional organizational structure shown in the attached organization chart (Annex 2).

The **most sensitive processes** which COIMA has identified internally are essentially the operating functions through which the company performs its business.

The organization chart shows the functions/operating processes in which the offences might occur. These functions/processes are identified using the **same nomenclature** as used inside COIMA and shown in the company's organizational structure.

Briefly the **positions/functions** at risk are:

- Managing Director;
- Financial & HR Director;
- Information Technology;
- Marketing & Dev. Mgr;
- Property Management;
- Project & Construction Management.

2.1. Goals and adoption of the Model

COIMA is conscious of the need to disseminate and consolidate a culture of transparency and integrity, and of the importance of guaranteeing conditions of fairness in the conduct of its business activities to protect its standing and reputation and meet the expectations of the shareholder; it therefore adopts the Organizational, Management and Control Model foreseen by Decree to specify the underlying principles.

2.1.1 Aims of the Model and its cardinal points

Adoption of the Model, while not required by the Decree³¹, is also intended to ensure that all who work for, or on behalf of, the company adhere to correct and transparent practices in the fulfilment of their duties, and thus avoid the risk of committing the offences foreseen by the Decree.

The main aim of the Model is to put in place a structured and organic system of procedures and controls designed to prevent, as far as possible, any conduct likely to lead to the commission of the offences contemplated by the Decree.

By identifying the activities exposed to a risk of crime ("**sensitive activities**") and introducing relevant procedures, we intend:

- first, to ensure that all those who work for, and on behalf of, COIMA, are fully aware of the risks of committing a crime punishable by law and strongly prohibited by the company as contrary to its interests in every case, even where it might appear to gain an immediate business advantage;
- second, through the constant monitoring of activities, to be able to act promptly to prevent or counter the commission of an offence.

Besides the above principles, the main features of the Model are:

³¹ Which recommends such a model as a voluntary but not obligatory measure.

- mapping risk activities, those areas of activity in which the commission of the crimes foreseen by the Decree is most likely, i.e. “sensitive activities”;
- charging the Supervisory Body with specific duties of oversight of the effectiveness and workings of the Model;
- inspection and documentation of every significant transaction;
- application and adherence to the principle of separation of duties, which ensures that no one has autonomous control over the whole process;
- attribution of powers coherent with organizational responsibilities;
- ex-post assessments of all corporate practices and the workings of the Model, with regular reviews;
- engagement and involvement of all company levels in implementing the codes of conduct, procedures and corporate policy.

2.1.2 Approval of the Model

The first draft of the Model was approved by the COIMA Board of Directors' resolution of 15 July 2009.

2.1.3 Amendments and revision of the Model

As established by the Decree, the Model was “issued by the governing body”³². Subsequent amendments and any substantial additions must therefore be approved by the Board of Directors of COIMA.

However, the Chairman of COIMA may - if requested by the Supervisory Body - make amendments or additions of a formal nature, such as changing the organization chart or amending chapter 1 following legislative reforms which alter the range of offences under the Decree, which do not have an impact on the sensitive activities of the company and the implementation of the new protocols.

2.2 Addressees of the Model

The rules enshrined in the Model apply to all those who perform functions of management, administration, direction or control within COIMA, the employees, and those who, while not employed by the company, operate on its behalf or are connected to it by contracting relations, consultancy or other agreements.

The Model shall be disseminated by such means as to ensure that all interested persons are fully informed.

All subjects addressed by the Model must adhere to its provisions in fulfilment of the duties of trust, fairness and diligence established by their legal relationships with the company.

COIMA condemns any conduct against the law, or contrary to the rules of the Model and the Code of Ethics, even where such behaviour is carried out in the interests of the company or with the intention of obtaining benefit for it.

3. Areas of risk

This section refers to practices by directors, executives, employees and senior officers of the company in the areas of activity at risk, as well as by external Contractors and Partners as defined above (hereinafter “Addressees”).

The purpose of this section is to ensure that all Addressees adopt the prescribed rules of conduct so as to prevent any occurrence of the offences foreseen by the Decree.

The main sensitive processes identified COIMA are listed below, in decreasing order of risk.

³² Article 6, paragraph 1, letter a) of the Decree.

3.1 Crimes against the Public Administration

Crimes against the Public Administration presuppose the establishment of relationships with the public administration: these relationships can be direct, indirect or occasional.

Direct relationships are those which involve unmediated contact between the company and a public function or a public service.

Indirect relationships are those involving activities complementary to or supporting a direct relationship with the Public Administration: for example, where a firm has an agreement with a local administration department which requires the services of COIMA, this is an indirect relationship; should the direct relationship between that firm and the Public Administration involve some form of bribery and corruption, the judicial authorities might take action against COIMA as well if it was found to be consciously and voluntarily complicit in the commission of crime against the Public Administration by the firm. COIMA will also monitor all potentially risky indirect relationships as far as possible.

Occasional relationships are those in which the PA carries out routine inspections of all companies operating in Italy within its various area of competence (health & safety, environment, labour, pensions, taxation etc.).

Based on its analyses, COIMA has only **indirect and occasional relationships with the Public Administration**.

The key sensitive processes identified to date by COIMA are listed below, in decreasing order of risk and divided into the two categories mentioned above:

Occasional relationships with the Public Administration:

- **Relationships with the PA regarding compliance with prevailing regulatory standards (urban planning, construction, pensions, compulsory and/or optional accident prevention, occupational health and safety obligations etc.) with special reference to PA controls and inspections.**
 - Corruption of judicial proceedings (article 319-ter of the Criminal Code)
 - Aggravated fraud at the expense of the state or another public body (article 640, paragraph 2, no. 1 of the Criminal Code)
 - Bribing a public official to do something (article 318 of the Criminal Code)
 - Bribing a public official not to do something (article 319 of the Criminal Code)
 - Improper inducement to a give or promise a benefit (article 319-quarter of the Criminal Code)
 - Incitement to corruption (article 322 of the Criminal Code)
- **Relationships with public bodies to obtain authorizations, licenses, permits to perform company business**
 - Bribing a public official to do something (article 318 of the criminal code)
 - Bribing a public official not to do something (article 319 of the Criminal Code)
 - Improper inducement to a give or promise a benefit (article 319-quarter of the Criminal Code)
 - Incitement to corruption (article 322 of the Criminal Code)
- **Assignment/management of positions, subcontracts and consulting contracts in relation to relationships with public bodies**
 - Bribing a public official to do something (article 318 of the Criminal Code)
 - Bribing a public official not to do something (article 319 of the Criminal Code)
 - Corruption of judicial proceedings (article 319-ter of the Criminal Code)
 - Improper inducement to a give or promise a benefit (article 319-quarter of the Criminal Code)
 - Incitement to corruption (article 322 of the Criminal Code)
- **Relationships with supervisory bodies in relation to regulated activities**
 - Bribing a public official to do something (article 318 of the Criminal Code)

- Bribing a public official not to do something (article 319 of the Criminal Code)
- Corruption of judicial proceedings (article 319-ter of the Criminal Code)
- Incitement to corruption (article 322 of the Criminal Code)
- Improper inducement to a give or promise a benefit (article 319-quarter of the Criminal Code)
- Embezzlement at the expense of the state (article 316-bis of the Criminal Code)

Indirect relationships with the Public Administration

▪ Management of liquidity and accounting

- Bribing a public official to do something (article 318 of the Criminal Code)
- Bribing a public official not to do something (article 319 of the Criminal Code)
- Incitement to corruption (article 322 of the Criminal Code)
- Corruption of judicial proceedings (article 319-ter of the Criminal Code)
- Improper inducement to a give or promise a benefit (article 319-quarter of the Criminal Code)
- Aggravated fraud at the expense of the state or another public body (article 640, paragraph 2, no. of the Criminal Code)
- Computer fraud at the expense of the state or another public body (article 640-ter of the Criminal Code)

▪ Assignment/management of positions and consulting contracts

- Bribing a public official to do something (article 318 of the Criminal Code)
- Bribing a public official not to do something (article 319 of the Criminal Code)
- Corruption of judicial proceedings (article 319-ter of the Criminal Code)
- Improper inducement to a give or promise a benefit (article 319-quarter of the Criminal Code)
- Incitement to corruption (article 322 of the Criminal Code)
- Aggravated fraud at the expense of the state or another public body (article 640, paragraph 2, no. 1 of the Criminal Code)

▪ Relationships with the financial authorities

- Bribing a public official to do something (article 318 of the Criminal Code)
- Bribing a public official not to do something (article 319 of the Criminal Code)
- Improper inducement to a give or promise a benefit (article 319-quarter of the Criminal Code)
- Incitement to corruption (article 322 of the Criminal Code)
- Aggravated fraud at the expense of the state or another public body (article 640, paragraph 2, no. 1 of the Criminal Code)
- Computer fraud at the expense of the state or another public body (article 640-ter of the Criminal Code)

▪ Management of gifts and donations to public officials

- Bribing a public official to do something (article 318 of the Criminal Code)
- Bribing a public official not to do something (article 319 of the Criminal Code)
- Incitement to corruption (article 322 of the Criminal Code)
- Corruption of judicial proceedings (article 319-ter of the Criminal Code)
- Improper inducement to a give or promise a benefit (article 319-quarter of the Criminal Code)

▪ Management of hiring and system of rewards

- Bribing a public official to do something (article 318 of the Criminal Code)
- Bribing a public official not to do something (article 319 of the Criminal Code)
- Incitement to corruption (article 322 of the Criminal Code)
- Corruption of judicial proceedings (article 319-ter of the Criminal Code)
- Improper inducement to a give or promise a benefit (article 319-quarter of the Criminal Code)

3.2 Corporate offences

The company performs most at risk activities on the basis of specific written procedures which are subject to period reviews and controls.

The areas of activity most specifically at risk in relation to corporate crime are the following:

- **Accounting, drafting of the financial statements, reports and company communications in general, and fulfilment of its statutory disclosure obligations**
 - Misleading corporate communications (article 2621 of the Civil Code)
 - Company communications which mislead shareholders or creditors (article 2622, paragraphs 1 and 2, of the Civil Code)
- **Managing corporate transactions and relations with shareholders and the Board of Statutory Auditors and preparing, keeping and storing the documents on which such may exercise control**
 - Unlawful allocation of profits and reserves (article 2627 of the Civil Code)
 - Improper repayment of contributions (article 2626 of the Civil Code)
 - Fictitious formation of capital (article 2632 of the Civil Code)
 - Transactions prejudicial to the creditors (article 2629 of the Civil Code)
 - Failure to disclose conflicts of interest (article 2629-bis of the Civil Code)
 - Obstructing control (article 2625, paragraph 2, of the Civil Code)
- **Activities relating to meetings of corporate bodies**
 - Unlawful influence on the Shareholders' Meeting (article 2636 of the Civil Code)
 - Obstructing control (article 2625, paragraph 2, of the Civil Code)
 - Unlawful allocation of profits and reserves (article 2627 of the Civil Code)
 - Fictitious formation of capital (article 2632 of the Civil Code)
 - Transactions prejudicial to the creditors (article 2629 of the Civil Code)
 - Failure to disclose conflicts of interest (article 2629-bis of the Civil Code)
- **Managing and communicating information and data externally**
 - Stock manipulation (article 2637 of the Civil Code)
 - Misleading corporate communications (article 2621 of the Civil Code)
 - Company communications which mislead shareholders or creditors (article 2622, paragraphs 1 and 2, of the Civil Code)
 - Obstructing control (article 2625, paragraph 2, of the Civil Code)
- **Acquisition of new clients and managing newly acquired customers on its own, or third parties', behalf**
- **Assignment/management of positions and consulting contracts (purchasing cycle)**
- **Management of liquidity and accounting**
- **Management of gifts and donations**
- **Management of hiring and system of rewards**
 - Bribery of private individuals (article 2635 of the Civil Code)³³

3.3 Manslaughter and serious/very serious injury through negligence committed in breach of the occupational accident prevention and health and safety regulations

Based on the company's analysis of the key sensitive activities, the most significant risk for COIMA appears to derive from the activities of subcontractors on building sites, the presence of COIMA personnel at these sites, and the use of computer terminals in the offices. Detailed assessments have been made of the risks pursuant to article 17, paragraph 1, letter a) of Legislative Decree no. 81/2008.

It is worth noting, however, that COIMA must constantly verify that all subcontractors, even those indirectly associated with COIMA companies, do observe all health and safety standards.

³³ Some sensitive areas overlap with those relating to offences against the Public Administration.

Listed below are the key safety risks identified by the company:

- **Health and safety risks in the workplace with particular reference to the following:**
 - Updating of the risk assessment report by (internal and external) managers to ensure they comply with Legislative Decree no. 81/2008;
 - Fulfilment of the training and information obligations pursuant to articles 36 and 37 of Legislative Decree no. 81/08.
 - Manslaughter (article 589 of the Criminal Code)
 - Personal injury through negligence (590 of the Criminal Code)

3.4 Computer crime

Based on company analysis and interviews with management in the IT department, the risk of cybercrime is not particularly high as the work does not involve intensive use of computer systems. The only risk area is that related to the observance of the minimum data processing security standards; failure to observe these rules could facilitate unauthorized intrusions to LAN and WAN networks and allow access to workers' individual personal computers.

- **Management of IT systems, databanks and networks in accordance with the security measures prescribed for computer data processing stated in the technical guideline for minimum security measures with particular reference to the following activities at risk;**
 - Use and management of the mailing list;
 - Protection of corporate data from intrusion or interception (keyloggers, backdoors);
 - Verification of the use of passwords to copyright-protected software and the presence of malicious software;
 - Unauthorized access to an IT system (article 615-ter of the Criminal Code);
 - Interception, impediment or unlawful discontinuation of IT or telemetric communications (article 617-quarter of the Criminal Code);
 - Installation of equipment to intercept, prevent or interrupt IT or telemetric communications (article 617-quinquies of the Criminal Code);
 - Possession and illicit circulation of passwords to computing or telemetric systems (article 615-quarter of the Criminal Code).
- **Training and online dissemination of documentation addressed to the Public Administration or private individuals**
 - Falsification of IT documents (article 491-bis of the Criminal Code);

3.5 Other types of crime

Regarding the other types of crimes foreseen by the Decree - abuse of inside information and market manipulation, money laundering and the recycling of money, assets or benefits of unlawful origin, forgery, offences against the person (slavery and child pornography), terrorist crime or subversion of the democratic order, transnational offences, organized crime, crimes against trade and industry, breach of copyright, inducing someone to make a false statement or commit perjury, environmental crime and employment of foreign citizens without valid stay permits - the risks are deemed to be negligible and, as a result, no specific rules or procedures have been put in place, without prejudice to the requirement of conduct adherent to the regulations and general standards of practice which inspire this Model.

3.6 Additional areas of risk

Any additions to the aforesaid areas of risk or "sensitive activities" shall be made, after prior consultation with the Supervisory Body, by the Board of Directors which is alone responsible for introducing the appropriate measures.

4. Procedures and principles of control

4.1 Crimes against the Public Administration

4.1.1 General codes of practice prescribed for the at risk areas of activity

This section sets out the express obligation upon Company Members³⁴ directly, and, by means of specific contractual clauses, external Contractors and Partners, to:

1. Strictly observe all laws and regulations governing company activity, with particular reference to activities involving contact and relationships with the Public Administration, a public function or a public service;
2. Managing relationships with the Public Administration in line with the principles of maximum propriety and transparency.

This section therefore expressly prohibits Company Members and, by virtue of specific contractual clauses, external Contractors and Partners, from entertaining:

1. practices likely to lead to commission of the offences considered above (articles 24 and 25 of the Decree);
2. practices which, though not themselves constituting the offences described above, might potentially lead to them;
3. any conflict of interest with the Public Administration related to the aforesaid crimes.

As part of such conduct, the **following are specifically prohibited**:

- **performing services in favour** of outsourcers, consultants, partners or contractors in general that are not suitably justified within the contractual relationship, or in relation to the type of work to be performed and current local practice;
- **making cash payments** or granting benefits of any nature (for example promising employment) in favour of public officials;
- **making gifts or giving presents** beyond established business practice, meaning any form of gift exceeding normal commercial or courteous practice or in any case designed to obtain favourable treatment in conducting any business activity. In particular, it is forbidden to give any form of gift to Italian and non-Italian public officials, or to their relatives, that may affect their discretion or independence of judgment or induce them to provide any benefit for the Company. COIMA corporate policy states that only gifts of little value are permitted. All gifts - except those of little value - must be suitably documented so that the Supervisory Body may conduct its inspections.

To prevent the above conduct:

- all **relationships with the PA** in at risk areas of activity must be dealt with on an individual basis, identifying the person in charge for each of the operations or sets of operations (in the event of repetition) carried out in the areas of activities at risk;
- **there must be a segregation of duties** founded on a separation between those who authorize, carry out and control the activities;
- the company must have **formal procedures** which provide codes of conduct and a modus operandi to carry out sensitive activities, plus procedures for the archival of important documentation;
- the **powers of signature and authorization** must be coherent with these formal procedures and clearly defined;
- all transactions relating to sensitive activities and the decision-making process must be **traceable**, and authorization and the performance of sensitive activities must be verifiable ex-post via paper or digital documentation;

³⁴ The term Company Members shall mean senior officers, directors and employees working within COIMA on any basis.

- **engagements with external contractors** in whatsoever capacity must also be formalized in writing, stating the agreed fee, and must be proposed or verified or approved by at least two members of COIMA.

The above shall hold without prejudice to any procedures of increased protection prescribed within COIMA for performing activities in the areas at risk.

4.1.2 Specific procedures for sensitive areas

Corporate procedures and practices already in place today governing sensitive activities and support processes are designed to prevent the commission of offences and incorporate the “principles of control” outlined below. These principles of control set out the requisites of the organizational – procedural system to ensure compliance with law/standards/procedures and guarantee effectiveness and efficiency.

Thus the prevention of crime through the adoption of this Organizational Model must be based on:

- **constant verification of** compliance with company procedures and the various levels of authorization/control³⁵;
- of the **reinforcement and removal** of any critical points found in the current organizational structure and which the Model is designed to eliminate.

Specific indications for each of the sensitive areas are given below.

Occasional relationships with the Public Administration:

- 1) **Relationships with the PA regarding compliance with prevailing regulatory standards (urban planning, construction, pensions, compulsory and/or optional accident prevention, occupational health and safety obligations etc.) with special reference to PA controls and inspections.**
- 2) **Relationships with public bodies to obtain authorizations, licenses, permits to perform company business**
- 3) **Assignment/management of positions, subcontracts and consulting contracts in relation to relationships with public bodies**
- 4) **Relationships with supervisory bodies in relation to regulated activities**

For each of the four above areas:

- protocols must be put in place governing the way in which persons in charge shall be involved in judicial, fiscal, administrative and/or supervisory inspections and the handling of relationships with public occupational safety and environmental protection officials both during inspections/controls and in the operational phases carried out to obtain authorizations, licenses or other items, through:
 - i) definition of roles/responsibilities, identifying the people or functions which can act as part of the activities;
 - ii) regulation of relevant phases (such as: reason for request/application and drafting of the necessary documentation, including with the help of outside entities/verification of documentation and signing of request etc.) and tracking of all stages;
 - iii) procedures must be introduced for the archival of important documentation;
- during any judicial, fiscal or administrative inspection or by the industry regulator (e.g. inspectors appointed to verify observance of Legislative Decree no. 81/08, taxation, INPS, health and municipal obligations) and any application for authorizations, licenses or permits, only those **expressly delegated to this task (at least two)** may take part. **Reports must be drawn up and filed** relating to the whole of the proceeding regarding the inspection. Should the minutes reveal any critical issues, the Supervisory Body must be informed in writing by the head of the department involved;

³⁵Note that as a consequence, the ability of the Supervisory Body to function properly basically depends on checking that the business procedures for each critical process identified are being complied with, covering all the critical phases involved in the Company's operations on a regular basis, in a rotational manner and using sampling. These aspects hold “for any operational phase in which COIMA is the main player” and accordingly by checking the activity of the parties involved and the authorizations received at the various operational levels.

- at least **two people belonging to the company** should take part in the inspection, preferably from **different functions**;
- dealings with the Public Administration must be **tracked and verified ex-post** through proper documents/reports;
- any **findings/issues** must be immediately brought to the attention of the Chairman and the Supervisory Body;
- controls must be introduced to **make sure that the organizational, management and control Model and other COIMA procedures are known** to all corporate functions through periodic information-training programmes for directors, senior staff and employees on offences against the Public Administration and the sanctions;
- the appointment of outsourcers, consultants, partners and contractors in general must be made using **transparent methods** in accordance with specific company procedures;
- **engagements with external Contractors (for example engineers for preparing the technical documentation required to renew authorizations and licenses) must also be formalized in writing**, stating the agreed fee, and must be proposed or verified or approved by at least two members of COIMA;
- the above agreements must contain **standard clauses** in which unconditional acceptance is given by the counterparties involved of the Legislative Decree no. 231/2001 Model established in COIMA;
- a **suitable declaration** must be included in agreements with outsourcers, consultants, partners and contractors in general in which they state that they are aware of the provisions of Legislative Decree no. 231/2001 and its implications for the Company and that they undertake to comply with Legislative Decree no. 231/2001;
- contracts with outsourcers, consultants, partners and contractors in general must contain a **clause governing the consequences** of a breach of Legislative Decree no. 231/2001 (e.g. express termination clauses, penalties);
- no type of **payment may be made in cash or in kind**;
- consultancy services provided **as per engagements, for example to technical experts**, must only contain the absolute truth. To this end a **suitable disclaimer** must be issued to COIMA as to the propriety of the documents produced and the fact that that the preparation and drafting of such documentation observed standards of the utmost **clarity, completeness and accuracy of the information indicated and sent to the Public Administration**;
- checks must be made for any **conflicts of interest** in the aforementioned relationships with the Public Administration. In this respect it is necessary to check for the existence of statements of grounds for incompatibility made by Company Members, including after such relationships;

Indirect relationships with the Public Administration

1) Management of liquidity and accounting

For sensitive areas the following requirements must be met:

- checks must be made to make sure that agreements, purchase orders, invoices and payments correspond, also with regard to **tax and national insurance amounts**, paying special attention to signed authorizations and the permitted spending limits;
- **reports, cash flows and bank statement reconciliations** must be verified³⁶;
- controls must be made of **company documentation** and **invoices payable**;
- **checks must be made on payment that the amount corresponds to the invoice or contract.**

Also:

- checks must be made to make sure that **agreements, purchase orders, invoices and payments correspond**, also with regard to **tax and national insurance amounts**, paying special attention to signed authorizations;

³⁶ In particular, for the cycle of receipts and payments behind the cash flows and bank reconciliations, all activity (as specified in the guidelines), must be registered, documented and immediately verifiable. In no case may there be undocumented movements of the company's financial resources. Cash must be kept in a safety deposit box in the custody of named individuals. It is expressly forbidden to invoice work that has not been done, issue duplicate invoices, or fail to issue a credit note where duplicate invoices have been issued in error for work that is fictitious, wholly or in part.

- verification of the **correspondence between payments made to contractors and members of corporate bodies** and the work effectively performed, which shall be fully documented;
- there must be **controls in place on reports, cash flows and bank statement reconciliations**;
- officers responsible for control and oversight of the obligations inherent in the above activities must report **any irregularities or anomalies** to the Supervisory Body; in particular regarding:
 - payment of invoices;
 - payments of sums payable to the tax and national insurance agencies;
 - correspondence between agreements, purchase orders and invoices;
 - allocation of funds received from EU, national or regional agencies, etc.

2) Assignment/management of positions and consulting contracts

With reference to sensitive areas the following procedures must be followed:

- the pre-appraisal and RFP procedures in the selection of suppliers;
- where employees, contractors, consultants and partners are required to conduct relationships with public officials on COIMA's behalf, **powers must be formally granted** (via specific proxy for employees or an ad hoc clause for the other subjects mentioned). Where necessary, the aforesaid subjects shall be given written power of attorney which complies with all the criteria specified;
- the choice of outsourcers, consultants, partners and contractors in general must be made using **transparent methods** in accordance with specific company procedures requiring final approval by the Chief Executive Officer;
- procedures for the selection and appraisal of suppliers must be verified in full, including the **choice of suppliers, receipt, evaluation and approval of offers**, invoicing and VAT accounting;
- a **clear separation of duties must be made between the various functions involved in the purchasing process**, in particular between the identification and choice of suppliers, consultants or providers, approval of the purchase order, authorization of payment and management control and tracking of the transactions;
- identify **general and transparent rules to determine the maximum price** of a product or service, including obtaining several quotes;
- general rules must be defined especially on **terms and conditions of payment**;
- **benchmarking** against market prices must be planned;
- the Supervisory Body must be informed in writing of any:
 - *purchases made at non-market prices* which do not comply with company standards;
 - *transactions for receipts at less than standard payment terms* (for example invoices paid on sight);
- contracts for services must **correspond exactly** with the services actually rendered; contracts between COIMA and outsourcers, consultants or partners must be drawn up in writing containing all terms and conditions and comply with the following points:
 - the above agreements must contain **standard clauses** in which unconditional acceptance is given by the counterparties involved of the Legislative Decree no. 231/2001 Model established in COIMA; in the absence of a contract, a specific 231 report must be contained within the purchase order;
 - a **suitable declaration** must be included in agreements with outsourcers, consultants, partners and contractors in general in which they state that they are aware of the provisions of Legislative Decree no. 231/2001 and its implications for the Company and that they undertake to comply with Legislative Decree no. 231/2001;
 - contracts with outsourcers, consultants, partners and contractors in general must contain a **clause governing the consequences** of a breach of Legislative Decree no. 231/2001 (e.g. express termination clauses, penalties);
- where employees, consultants, partners and contractors in general are required to conduct relationships with public officials on COIMA's behalf, **powers must be formally granted** via a specific contractual clause.

3) Relationships with the financial authorities

For sensitive areas the following requirements must be met:

- protocols must be drawn up to govern **participation in judicial, fiscal, administrative or regulatory inspections**;
- during any judicial, fiscal or administrative inspection or by the industry regulator (e.g. inspectors appointed to verify observance of Legislative Decree no. 81/08, taxation, INPS) only those **expressly delegated to this task** (at least two) may take part. **Reports must be drawn up and filed** relating to the whole of the proceeding regarding the inspection. Should the minutes reveal any critical issues, the Supervisory Body must be informed in writing by the head of the department involved.

4) Management of gifts and donations to public officials

For sensitive areas the following requirements must be met:

- **corporate procedure must be defined on** gifts, promotions and advertising, donations and entertainment expenses containing, among other things, the following elements: i) definition of the roles/responsibilities of the subjects involved; ii) limits on the value of the gifts, donations, entertainment and promotional expenses; iii) clear and precise criteria for the selection of the initiatives funded; iv) conservation of important documentation; v) a list of subjects in receipt of gifts, donations or entertainment expenses specifying the PA officials and the gift or expense for each beneficiary;
- **special authorization** must be required to make gifts, sign advertising or sponsorship agreements and cover entertainment expenses;
- forbid **gifts of money or benefits of any kind** (e.g. promises of employment) to public officials responsible for occupational accident prevention and health and safety inspections;
- ensure that the **Model and information-training programmes** on the requirements of the Decree are known to all company Contractors in general;
- forbid the **distribution of gifts and presents other than those permitted by corporate procedure**. In particular, it is prohibited to give gifts of any kind to Italian or foreign public officials, or their relatives, which might influence their discretion or independence of judgement or induce them to favour the company;
- verify that the cost of gifts or entertainment and promotional expenses fall within the **annual budget approved** for promotional activities for the specific area of business;
- **verify compliance** with the principles and procedures specified in the **Code of Ethics**.

5) Management of hiring and system of rewards

For sensitive areas the following requirements must be met:

- **formalize a corporate procedure** for the hiring of personnel which foresees, among other things, the following: i) objective and transparent selection criteria (e.g., degree/diploma grades, knowledge of foreign languages, previous work experience, etc.); ii) definition of roles and responsibilities for the subjects involved involving two people in the choice of candidate and in the assessment/promotion of the employee; iii) procedures defined for the archival of important documentation;
- ensure the **archiving of documents justifying the selection/hiring/promotion process**, giving reasons and attesting to the appropriateness of the decision, and correct hierarchical approval;
- set up **bonus schemes** incorporating predetermined, measurable and "feasible" targets involving multiple functions in the drawing up of incentive plans and the identification of beneficiaries.

For sensitive areas the following requirements must be met:

- clear **definition of the roles and duties of the people responsible** for selection and management of employees and contractors;
- a **structured system to evaluate candidates** to ensure the traceability of the reasons for the choice/rejection of a candidate;
- identification of the **person responsible** for managing the tasks in question and the attribution of responsibilities;
- management of **incentives** for employees and contractors;
- definition of **methods of archiving documentation** relating to the tasks in question to ensure that they are readily available if requested and to track the process.

Equally:

- remuneration **systems must be monitored**;
- checks must be made to ensure that agreements, invoices and payments correspond, also with regard to **tax and national insurance amounts**, paying special attention to signed authorizations;
- compliance must be verified with **authorization powers, proxies, powers of attorney**, and possible conflicts of interest monitored, especially for persons having meetings or even indirect relations with the PA.

In addition:

- this Model should be **brought to the attention** of all personnel, not only management; using specific means communication (such as notices in common spaces and periodic publications) to inform everyone of changes or updates to the Model;
- managers are **responsible for the training and updating of their employees and contractors**;
- all personnel with executive powers of control and oversight over staff who work with the PA must monitor carefully the activity of their people and report any irregularities immediately to the Supervisory Body; they should also implement internal controls, including surprise inspections, to ensure that the accounting books are accurate and transparent.

4.2 Corporate offences

4.2.1 General codes of practice prescribed for the at risk areas of activity

This section expressly forbids Addressees to:

- conduct themselves, collaborate or cause conduct to be carried out in such a way that it falls within the scope of the above-mentioned offences (article 25-ter of the Decree);
- conduct themselves, collaborate or cause conduct to be carried out in such a way that although their conduct does not of itself represent one of the above-mentioned offences, it may potentially lead to one.

This section therefore expressly requires Addressees to be aware of and comply with the following:

- the principles of Corporate Governance approved by the corporate bodies of COIMA incorporating prevailing standards;
 - company standards inherent to the administrative, accounting, financial, and reporting system;
 - company standards inherent to the use and functioning of the COIMA IT system;
- applicable regulations in general.

As part of such conduct it is **absolutely mandatory** to:

- maintain correct, transparent and collaborative conduct towards compliance with the law and internal business procedures in all activities whose scope is the preparation of the annual financial statements and other company communications, to provide the shareholders and third parties with a truthful picture of the Company's business, equity and financial position;
- maintain correct, transparent and collaborative conduct towards compliance with the law and internal business procedures in the acquisition, processing and communication of the data and information required to form a reliable assessment of the Company's business, equity and financial position and the evolution of its business activities;
- comply strictly with all provisions of the law designed to protect the integrity and effectiveness of the share capital, to avoid damaging the guarantees of creditors and third parties in general;
- guarantee the normal functioning of the company and the corporate bodies, safeguarding and facilitating every form of internal control over company management;
- desist from making fictitious or otherwise fraudulent transactions, or disseminating false or incorrect information which might significantly distort the business/equity/financial results of COIMA;
- make all legally required disclosures with timeliness, propriety and **in good faith**.

As part of such conduct, it is also **specifically forbidden** to:

- present or transmit for preparation of the annual statements or reporting package, false or incomplete reports and statements or communications or which in any case do not truthfully reflect the Company's business, equity and financial position;
- omit data and information mandatory by law on the Company's business, equity and financial position;
- repay contributions to shareholders or release them from their obligation to make them, except in cases of a legitimate reduction in the share capital;
- distribute profits or advances on profits which have not been effectively earned or which are destined by law for reserves;
- implement reductions in share capital, mergers or spin-offs in breach of the legal protections for creditors, thereby causing damage to the same;
- make an artificial formation or increase in share capital, attributing quotas or shares for less than their par value during a capital increase;
- engage in **obstructive behaviour**, either by concealing documents or by other fraudulent means, designed to impede the activities of control and review by the entity responsible for the statutory audit of the accounts pursuant to articles 2409 et seq. of the Civil Code;
- engage in any behaviour which might obstruct the work of the supervision and control, including inspections by the public authorities (revenue agency, labour inspectors, etc...) for example oppose, refuse, obstruct or fail to collaborate such as by delaying communications of available documents, failing to attend meetings at the prearranged time.

In addition the following controls are required:

- implementation of information-training courses for personnel involved with the rules of corporate governance and of corporate crime;
- arrangement of regular meetings between the control functions of the Company and the Supervisory Body to check observance of the rules of corporate regulation and corporate governance (including the issue of a certificate of attestation);
- delivery to all control functions - with reasonable notice – of all documents relating to matters on the agenda of meetings of the corporate bodies or on which they are required to express an opinion.

4.2.2 Specific procedures for sensitive areas

In addition to the general principles contained in this Model, the following specific procedures for the individual sensitive areas must also be complied with in order to implement the rules listed in the previous paragraph.

1) Preparation of the annual financial statements, reports and other corporate communications required by law (data presentation, processing and approval)

Communications and/or documents (for example **annual financial statements**) must be prepared on the basis of special business procedures that:

- **establish clearly and completely the data and information** that each function must provide, the accounting policies to be used for data processing and a timetable for delivery to the functions in charge;
- provide for the **transmission of the data and information to the function in charge by means of a computer or other system** that enables individual steps to be tracked and the persons entering the data in the system to be identified;
- provide for **regular meetings and/or exchanges of information with any accountancy, fiscal, etc. outsourcers** to ensure that the service is being performed and the accounting documents are being prepared in a proper and constant professional manner;
- use **budgeted information agreed** by the functions involved and approved by the Corporate Bodies;
- establish that **changes to the accounting data** may only be made by the function generating such data.

2) Managing corporate transactions and relations with shareholders and the Board of Statutory Auditors and preparing, keeping and storing the documents on which such may exercise control

Corporate transactions and relations with shareholders and the Board of Statutory Auditors must be handled on the basis of specific business procedures which provide for the following:

- checks that internal **corporate governance and code of ethics** rules are being complied with;
- **controls over the dispatch of economic and financial operational reports** to the Board of Directors, over cash flows and over bank reconciliations, on the basis of the requirements of the management control system and the relative operational indicators **liable** to anomalies in the functioning of the rules of good corporate governance;
- **the requirement to hold one or more meetings between the Board of Statutory Auditors and the Supervisory Body** whose object is to ensure compliance with company law and corporate governance legislation as well as compliance by directors, management and employees in their resulting conduct;
- controls designed to **check that all business functions are actually aware** of the Organizational Model, including by way of regular information-training courses attended by directors, senior officers and employees in general on corporate criminal offences and the relative sanctioning schemes;
- controls **over the system of communications, including that involving external communications**, in which an announcement is made to the market and to COIMA's main interlocutors that the Company has adopted the 231/2001 Model for the prevention of the criminal offences provided by the law and that COIMA accordingly gives considerable emphasis to an ethical approach;
- controls **over the system for communicating powers and proxies externally** and checking that such are complied with and over **powers of authorization, conflicts of interest and related parties**;
- **the requirement to provide the Board of Statutory Auditors** – with reasonable notice – with all the documents relating to matters on the agenda of meetings of shareholders or the Board of Directors on which the Board of Statutory Auditors is required to express an opinion.

3) Activity relating to meetings of the corporate bodies

Activity relating to shareholders' meetings must be handled on the basis of specific business procedures which provide for the following:

- the formalization of controls that **meetings of shareholders and the Board of Directors are held** on the basis of the Company's bylaws;
- **the definition of roles and responsibilities** relating to the preparation of preliminary documentation, the transcription and publication of the minutes of shareholders' meetings and board meetings and the retention of the register of the meetings and resolutions of shareholders and the Board of Directors.

Reference should be made to article 2391 of the Civil Code for the means of dealing with any conflicts of interest.

4) Managing and communicating information and data externally

Information and data externally must be handled and communicated on the basis of specific business procedures which provide for the following:

- **the definition of roles and responsibilities** in handling and coordinating the Company's communications and external relations;
- **the existence of formalized restrictions** (e.g. Company regulations or internal circulars, contractual clauses) as a means of maintaining the utmost confidentiality concerning data/information/documents acquired by employees and/or external consultants/contractors during the course of work performed for the Company;
- **the existence of suitable security measures for computerized data processing**, such as those to be found in Legislative Decree no.196/2003.

4.2.3 Specific procedures for sensitive areas – corruption between private parties

To prevent the offence of corruption between private parties being committed pursuant to article 2635 of the Civil Code in the capacity of corrupter the general protocols below must be followed:

The Addressees are expressly prohibited from:

- giving or promising money or other benefits to directors, general managers, managers in charge of the preparation of corporate accounting documents, statutory auditors and liquidators of corporate customers or potential corporate customers in the private sector;
- assuming conduct which, although not such to constitute in itself a criminal act pursuant to article 2635 of the Civil Code, may possibly become one;
- finding themselves in or giving rise to a situation of conflict of interest with respect to their customers or potential customers in relation to such offence.

As part of such conduct the following **are specifically prohibited**:

- **performing services in favour** of outsourcers, consultants, partners or contractors in general that are not suitably justified within the contractual relationship, or in relation to the type of work to be performed and current local practice;
- **making cash payments** or granting benefits of any nature (for example promising employment) in favour of the parties stated in article 2635 of the Civil Code;
- **making gifts or giving presents beyond established business practice**, meaning any form of gift exceeding normal commercial or courteous practice or in any case designed to obtain favourable treatment in conducting any business activity. In particular, it is forbidden to give any form of gift to Italian and non-Italian public officials, or to their relatives, that may affect their discretion or independence of judgment or induce them to provide any benefit for the Company. As provided by COIMA's business policies, permitted gifts are always characterized by their low value. All gifts - except those of little value - must be suitably documented so that the Supervisory Body may conduct its inspections.

To prevent the above conduct:

- **engagements with external contractors** in whatsoever capacity must also be formalized in writing, stating the agreed fee, and must be proposed or verified or approved by at least two members of COIMA;
- **no type of payment may be made in cash or in kind**;
- anyone **performing a control and supervisory function** over procedures connected with carrying out the above activities (the payment of invoices, the allocation of funds obtained from the state or community bodies) must place particular emphasis on the implementation of these procedures and report any irregularities immediately to the Supervisory Body.

In addition to these overall general principles, the following specific procedures must also be complied with for the individual sensitive areas:

5) Managing the process for the acquisition of new customers and managing acquired customers on the Company's behalf and on behalf of third parties

The protocols below must be followed to monitor this sensitive area:

- a clear segregation of duties and responsibilities must exist which regards on the one hand the powers for authorizing the processes of identifying and managing customers on the Company's behalf and on behalf of third parties and on the other powers for authorizing spending;
- a clear-cut allocation of duties must exist between the various functions as part of the organization of the process for stipulating new contracts or contractual renewals, in particular between responsibilities for customer relations (account manager), responsibilities for defining the offering price and the payment conditions and timing (and related penalties) and responsibilities in determining settlements in the case of any disputes;
- a clear-cut allocation of duties must exist between the various functions as part of the organization of the purchasing cycle, in particular between the function that identifies and selects the supplier, consultant or service provider, the function that approves the purchase order, the function that authorizes the payment and the function that carries out management control and the traceability of transactions;
- general and transparent criteria must be set for determining the maximum offer price by individual service so that any anomaly may be easily identified;
- general rules must be established in particular for payment terms and conditions;
- benchmarking against market prices must be planned;

- suitable Company protocols must be prepared for: the purchase of goods and services and the assignment of engagements for consultancy and other professional services;
- the Supervisory Body must be notified of the following:
 - contracts arranged for amounts exceeding a given amount that represents the risk threshold;
 - all transactions for receipts at less than standard payment terms (for example invoices paid on sight);
 - *no type of payment made be made in **cash** or in **kind***;
- *check for the existence of any **conflicts of interest** in dealing with the above relationships with private third parties. In this respect it is necessary to check for the existence of statements of grounds for incompatibility made by Company Members, including after such relationships;*
- *to this end formalize controls designed to ensure that all the business functions are actually aware of the Organizational, Control and Management Model and the **Code of Ethics** including by way of regular information-training courses attended by directors, senior officers and employees in general on offences involving corruption and the relative sanctioning schemes;*
- ensure that powers of authorization, delegated powers, proxies and possible conflicts of interest, especially regarding people that hold meetings and/or have relationships with private third parties, are being complied with by performing procedures on a sample of the signed documentation.

6) Assignment/management of engagements and external consultancy (purchasing cycle)

7) Management of liquidity and accounting

8) Management of gifts and donations

9) Management of hiring and system of rewards

The same control standards also apply to offences against the Public Administration for each of the above sensitive areas, to the extent compatible.

4.3 Manslaughter and serious/very serious injury through negligence committed in breach of the occupational accident prevention and health and safety regulations

4.3.1 General principles of conduct prescribed in the area of activities at risk

As part of the new types of crime introduced by article 9 of Law no. 123 of 3 August 2007, “**Measures on occupational health and safety**”, the provisions of Legislative Decree no. 231/2001 were supplemented by the legislative provision included in article 25-septies of that decree, regarding the offence of *manslaughter and serious/very serious injury through negligence committed in breach of the occupational accident prevention and health and safety regulations*”.

With the introduction of the Consolidated Law on Safety by way of Legislative Decree no. 81/2008, there are now specific requirements that must be included in organizational and management Models.

To this end this section requires the following to be performed:

- **compliance of** equipment, plant, workplaces and chemical, physical and biological agents **with legal technical-structural standards**;
- **risk assessment procedures** with the resulting introduction of **prevention and protection measures**;
- activities of an **organizational nature**, such as dealing with emergencies, first aid, tender management, regular safety meetings, discussions between the workers’ safety representatives;
- **health supervision** activities;
- workers’ **information and training** activities;
- **supervisory** activities regarding compliance by workers with safety procedures and instructions;
- the acquisition of **documentation and certifications** mandatory by law;
- regular checks that the adopted procedures are being applied and are effective.

This section additionally provides for the explicit requirement for Company Members³⁷ directly, and external Contractors and Partners by way of specific contractual clauses, to perform the following:

1. to comply with all the laws and regulations governing the Company's activity, with specific reference to **occupational accident prevention and health and safety regulations** in accordance with the **Uni-Inail Guidelines of 28 September 2001** or **British Standard OHSAS 18001/2007**;
2. to manage all relationships for applying **occupational accident prevention and health and safety** regulations, including those with the Public Administration, on the basis of the utmost propriety and transparency.

This section accordingly prescribes that Company Members directly, and external Contractors and Partners by way of specific contractual clauses, are expressly forbidden:

1. to behave in such a way that their conduct falls within the scope of the above-mentioned offences (article 25-septies of the Decree);
2. to behave in such a way that although their conduct does not of itself represent one of the above-mentioned offences, it may potentially become one;
3. to create any situation entailing a conflict of interest with respect to the Public Administration and/or any responsible authority in relation to the above-mentioned offences.

As part of such conduct, the following **are specifically prohibited**:

- **performing services in favour** of outsourcers, consultants, partners or contractors in general that are not suitably justified within the contractual relationship arranged with such, or in relation to the type of engagement to be performed and current local practice;
- **making cash payments** or granting benefits of any nature (for example promising employment) to public officials who may also be involved in carrying out controls in the sphere of **occupational accident prevention and health and safety** regulations;
- **making gifts or giving presents beyond established business practice**, meaning any form of gift exceeding normal commercial or courteous practice or in any case designed to obtain favourable treatment in conducting any business activity. In particular, it is forbidden to give any form of gift to Italian and non-Italian public officials, or to their relatives, that may affect their discretion or independence of judgment or induce them to provide any benefit for the Company.

In order to prevent the above-mentioned conduct occurring:

- **relations with the Public Administration and with the authorities** responsible for supervising occupational accident and health and safety regulations for the areas of activities at risk must be dealt with on an individual basis, identifying the person in charge for each of the operations or sets of operations (in the event of repetition) carried out in the areas of activities at risk;
- **engagements with external Contractors** in whatsoever capacity they may be performed, including those regarding occupational accident and health and safety regulations, must be formalized in writing, stating the agreed fee, and must be proposed or verified or approved by at least two members of COIMA;
- anyone **performing a control and supervisory function** over procedures connected with carrying out the above activities (the payment of invoices, the allocation of funds obtained from the state or community bodies) must place particular emphasis on the implementation of these procedures and report any irregularities immediately to the Supervisory Body.

The above shall hold without prejudice to any procedures of increased protection prescribed within COIMA for performing activities in the areas at risk.

4.3.2 Specific procedures for sensitive areas

The underlying assumptions for preventing offences through the adoption of the Organizational Model must be based on the following:

³⁷ The term Company Members shall mean senior officers, directors and employees working within COIMA on any basis.

- **continuous checks** of compliance with the internal procedures and the various levels of authorization controls prescribed in the specific checklists prepared by the Company which must be constantly updated³⁸;
- **reinforcement, strengthening and removal** of certain critical points that the organizational structure currently has and which the Model intends to eliminate.

In particular, for each of the sensitive areas/processes stated below:

- **Management of occupational health and safety risks with specific reference to the following activities:**
 - updating the “Risk Assessment Document” to be carried out by the persons in charge (internal and external) in order for this to comply with the requirements of Legislative Decree no. 81/2008;
 - the training and information requirements set out in articles 36 and 37 of Legislative Decree no. 81/08;

At a minimum the following procedures should be performed:

- document **procedures that govern the way in which persons in charge shall be involved in judicial, fiscal, administrative and/or supervisory inspections** and the way in which relations with public entities shall be managed, including persons in charge of safety at work, environmental protection, accident prevention regulations and occupational health and safety protection, during inspections/controls and in the operational phases carried out to obtain authorizations, licenses or other items;
- ensure that (at least two of) **the persons expressly delegated** are present during any judicial, fiscal and administrative inspections and those performed by the Supervisory Authorities of the sector concerned (such as for example those responsible for ensuring compliance with Legislative Decree no. 81/08), and in any action preliminary to the request for authorizations, licenses or other items. **Reports must be drawn up and filed** relating to the whole of the proceeding regarding the inspection, the authorization request or other matter. Should the report reveal any critical issues, the Supervisory Body must be informed in writing by the head of the department involved;
- check for the existence of any **conflicts of interest** with respect to personal relationships, ownership relationships, legal relationships or any other relationships existing with individuals or legal entities of the Public Administration with whom or with which COIMA’s personnel may establish relations regarding the sensitive areas in question (meaning during inspections/controls and during the application for authorizations, licenses, concessions and other items, with specific reference to accident prevention and occupational health and safety regulations);
- perform controls on the **documentation produced (in particular the Risk Assessment Document), including by any external technicians who may have been engaged, for the request for any type of authorization, license, concession or other item;**
- acquire and check the **documentation produced by contractors attesting compliance with safety regulations;**
- perform procedures to check the ex post **traceability and verifiability of transactions** carried out with the Public Administration by means of suitable document/information support including with reference to accident prevention and occupational health and safety regulations;
- **bring any findings or other issues** to the immediate knowledge of the Chairman as well as to the attention of the Supervisory Body;
- **to this end formalize controls designed to ensure effective awareness by all the Company’s functions and training programs in this respect regarding** the Organizational, Control and Management Model and COIMA’s other business procedures on accident prevention and occupational health and safety regulations. Carry out regular information-training courses attended by directors, senior officers and employees in general on safety at work and on the offences connected with the failure to comply with accident prevention and occupational health and safety regulations and the relative sanctioning and disqualification systems;

³⁸Note that as a consequence, the ability of the Supervisory Body to function properly basically depends on checking that the business procedures for each critical process identified are being complied with, covering all the critical phases involved in the Company’s operations on a regular basis, in a rotational manner and using sampling. These aspects hold “for any operational phase in which COIMA is the main player” and accordingly by checking the activity of the parties involved and the authorizations received at the various operational levels.

- **hold regular meetings** with the people in charge of safety at work, including those outside the Company, for the purpose of carrying out a constant analysis of their ability to keep safety at work measures updated over time in general and also on the basis of legislative changes;
- the outsourcers, consultants, partners and contractors in general dedicated to the procedures connected with accident prevention and occupational health and safety must be chosen using **transparent methods** and in accordance with a specific business procedure;
- **engagements with external Contractors (for example engineers for preparing the technical documentation required to renew authorizations and licenses or for complying with accident prevention and occupational health and safety regulations) must also be formalized in writing**, stating the agreed fee, and must be proposed or verified or approved by at least two members of COIMA;
- the above agreements must contain **standard clauses** in which unconditional acceptance is given by the counterparties involved of the Legislative Decree no. 231/2001 Model established in COIMA;
- a **suitable declaration** must be included in agreements entered with outsourcers, consultants, partners and contractors in general in which they state that they are aware of the provisions of Legislative Decree no. 231/2001 and its implications for the Company and that they undertake to comply with Legislative Decree no. 231/2001;
- a **clause governing the consequences** of any breach by them of the provisions of Legislative Decree no. 231/2001 (e.g. express termination clauses, penalties) must be included in agreements entered with outsourcers, consultants, partners and contractors;
- no kind of **payment may be made in cash or in kind**;
- consultancy services provided **as per engagements, for example to technical experts**, and relating to representation that COIMA is complying with accident prevention and occupational health and safety regulations in a proper and accurate manner must only contain the absolute truth. To this end a **suitable disclaimer** must be issued to COIMA as to the propriety of the documents produced and the fact that that the preparation and drafting of such documentation observed standards of the utmost **clarity, completeness and accuracy of the information indicated and sent to the authorities in charge of supervising compliance with accident prevention and occupational health and safety regulations** have been followed;
- procedures must be performed to identify any **conflicts of interest** in managing these relationships with respect to the consultants involved in the drafting and preparation of the technical reports to be sent to the authorities competent in matters concerning compliance with accident prevention and occupational health and safety regulations and to Company Members, including after such relationships.

4.4 Computer crime

4.4.1 General principles of conduct prescribed in the areas of activities at risk

This section expressly forbids the Addressees to perform the following:

- conduct themselves, collaborate or cause conduct to be carried out in such a way that it falls within the scope of the above-mentioned offences;
- conduct themselves, collaborate or cause conduct to be carried out in such a way that although their conduct does not of itself represent one of the above-mentioned offences, it may potentially become one.

This section consequently expressly requires Addressees to be aware of and comply with the following:

- the provisions of technical guidelines for minimum security measures with particular reference to the IT authentication and authorization system;
- all the measures designed to ensure the reliability of the system, also taking into account technical developments, concerning: the security of the processed data, the risk of destruction or loss and the risk of unauthorized or non-permitted access.

As part of such conduct, **the following are absolutely mandatory**:

- **to maintain correct, transparent and collaborative conduct** towards compliance with the law and internal business procedures in all activities whose scope is corporate communications;

- **to ensure** full compliance with laws and regulations and internal business procedures when acquiring, processing and **communicating data and information for legal purposes**;
- **to carry out on a timely basis**, correctly and **in good faith** all the communications to the Public Authorities required by laws and regulations with particular attention being given to those sent to the Italian Data Protection Authority, not obstructing the work performed by the supervisory departments of such bodies;
- **to check**, including by way of IT audits, **the consistency and reliability of the Company's information systems**, also with regard to the Company's reporting requirements to the supervisory authority;
- **to draw up effective security plans** and **perform systematic monitoring** of the Company's intranet with the aim of avoiding the commission of any offences.

4.4.2 Specific procedures for sensitive areas

For the purpose of implementing the rules listed in the previous paragraph the specific procedures below must be followed for individual sensitive areas, in addition to the general principles contained in this Model.

- Management of IT systems, databanks and networks in accordance with the security measures prescribed for computer data processing stated in the technical guideline for minimum security measures with particular reference to the following activities at risk;;
- Formation and electronic transmission of documentation addressed to the Public Administration or private parties.

The following are required for such sensitive areas:

- check that internal **data transmission** is assured by secure technological architecture (the existence of firewalls);
- check for the **existence of specific restrictive security measures** for internet connections (e.g. a blacklist);
- check for **the existence and effectiveness of back-up plans** in order to assure a complete and updated database for all possible contingencies, also from the standpoint of any inspections that may be performed by the supervisory authorities;
- using suitable electronic means **protect sensitive data against unauthorized access** by anyone entering the IT system by way of hardware or software tools (rootkits, sniffers, keyloggers, anonymizers, malicious software);
- **reporting by the functions concerned to the Supervisory Body on a timely basis cases where:**
 - the criteria established in the technical guidelines for the minimum IT security measures are being followed but transactions are being carried out that may undermine the effective protection of personal data or protection against intrusion into the Company's intranet.

5. Corporate Governance

5.1 General principles

The Company itself and the corporate bodies base their activity on the principles of correct corporate and business management as well as the principles established by the Code of Ethics.

This system of corporate governance is directed towards:

- maximizing shareholder value;
- customer service quality;
- transparency towards the market.

Role of the Board of Directors

The Board of Directors has the power and the duty to manage the business by pursuing a primary objective of creating value for the shareholder; to this end it assumes all the decisions necessary or useful for



achieving the Company's purpose.

1. Powers of the Board of Directors

Pursuant to the Company's bylaws the Board of Directors exercises all the powers of ordinary and extraordinary administration, exercising a general power of direction and control over the Company's activity and business operations; more specifically, the Board of Directors:

- a) examines and approves the Company's strategic, business and financial plans;
- b) reviews and approves the Company's annual budget;
- c) examines and approves the operations – including investments and divestments – which by their nature, strategic importance, size or the commitments they may cause, have a considerable effect on the Company's activity;
- d) checks the suitability of the Company's general organizational and administrative structure;
- e) assigns and removes the directors' powers, establishing limits, the means by which these powers are exercised and the frequency, usually not less than once every six months, with which the delegated bodies must report to the Board on the work performed in exercising the powers bestowed upon them;
- f) oversees operations in general, with specific attention being given to situations involving conflicts of interest, taking into particular consideration the information received from directors holding powers as well as carrying out a regular comparison between budgeted and actual results;
- g) exercises the other powers assigned to it by law and the Company's bylaws.

2. Duties of the directors

The directors bring to the Company the specific professional skills with which they are endowed; they are aware of the duties and responsibilities of the position; they dedicate the necessary time to it; they adopt resolutions in an informed manner; they keep the information acquired as part of their position confidential. The Chairman informs the Board of important legislative and regulatory changes that regard the Company and its corporate bodies.

3. Composition of the Board of Directors

The Board of Directors consists of executive directors (meaning directors to whom specific powers are assigned, including the Chairman) and non-executive directors having consultative functions.

If authorized officers are appointed they must be assigned specific powers in accordance with the principle of the segregation of powers.

4. Chairman of the Board of Directors

Without prejudice to the Company's bylaws, the Chairman of the Board of Directors:

- a) calls the meetings of the Board of Directors, sets the agenda and by way of preparation of the meetings, with due timeliness taking account of the specific circumstances, provides the directors with documentation that will enable them to participate in an informed manner at the sessions of the collegiate body;
- b) governs the proceedings of meetings and voting;
- c) regularly informs the Board about events of importance and, on at least a six-monthly basis, about the Company's general performance.

5. Meetings of the Board of Directors

The Board of Directors meets on a regular basis, at least every six months, and in any case when in the Chairman's opinion it is in the Company's interest; the Board also meets on the initiative of the directors and the Statutory Auditors, if appointed, pursuant to the law and the Company's bylaws.

Board meetings are chaired by the Chairman who is assisted by the Secretary who need not necessarily be a member of the Board of Directors.

Any director may propose matters for discussion at meetings of the Board of Directors; the Board decides whether and when the matter will be debated.

6. Delegated powers

The Board of Directors assigns powers to one or more of its members, establishing the nature and setting the respective limits, and may revoke such powers at any time.

Persons who due to their specific skills are capable of contributing to the adoption of resolutions that have been assessed from every standpoint and adopted for fully grounded reasons are called to be members of the Board of Directors.

The Board of Directors may assign specific duties to its members, establishing the nature and setting the respective limits and term.

As part of the assigned powers material operations, and in particular banking operations and the purchase and sale of fixed assets and equity investments exceeding certain fixed limits, must receive the approval of at least four directors as a means of ensuring effective control.

7. Internal control

The Company's internal control system is a process designed to ensure the efficient management of its corporate and business affairs; to make management decisions that are known and verifiable; to provide reliable accounting and operating information; to ensure compliance with laws and regulations from any source and protect the integrity of the Company's assets; and to prevent fraud against the Company, its shareholders and its corporate creditors.

8. Related party transactions

The Company's activity is based on principles of propriety and transparency. To this end, related party transactions must be carried out in accordance with criteria of substantial and procedural propriety.

9. Shareholders' meetings

The Company encourages and facilitates participation at shareholders' meetings and in particular provides all the information and documents required by shareholders for straightforward and knowledgeable participation.

5.2 The system of delegated powers and proxies

In principle, a system of delegated powers and proxies should be characterized by elements of "security" for the purpose of preventing criminal offences (tracking and traceability of sensitive transactions) while at the same time enabling business operations to be carried out efficiently.

"**Delegation**" means the act of assigning functions and duties, reflected in the system of organizational communication, while "**proxy**" means the unilateral legal act through which a company assigns powers of representation towards third parties.

A "**general proxy**" having a suitable scope consistent with the functions and powers assigned to the holder through "delegation" is granted to persons having a business function (generally senior officers who are not members of the board of directors) who in order to perform their duties need powers of representation.

The **essential requirements for a system of delegated powers** which can effectively prevent criminal offences are as follows:

- delegated powers must **link** each management power with the relative responsibility and with a suitable position in the organization chart and must be updated as the result of any organizational changes,
- each delegated power must state specifically and unequivocally:
 - **the powers delegated**;
 - the **body or individual to whom the holder of the delegated powers reports** hierarchically;
 - the **managerial powers assigned by way of the delegation**, and implementation must be consistent with the Company's purpose.



Holders of delegated powers must have **spending powers appropriate** for the duties assigned to them.

The **essential requirements for a system of assigning proxies** which can effectively prevent criminal offences are as follows:

- **general functional proxies** are only granted to persons holding an internal delegation that describes the relative management powers, and where necessary are accompanied by a suitable communication that sets the scope of powers of representation and possibly also spending limits.

An ad hoc procedure must **govern the means and responsibilities** for ensuring that proxies are updated on a timely basis, establishing the cases where these must be assigned, amended or revoked (e.g. on assuming new responsibilities, the transfer to other duties that are incompatible with those for which the proxy was assigned, resignation, dismissal, etc.).

On a regular basis, and with the support of other competent functions, the Supervisory Body **reviews the system of delegated powers and proxies** currently in force and its consistency with the whole organizational communications system (the documents within the Company by which delegated powers are assigned), recommending any changes in the event that the management power and/or position does not correspond to the powers of representation assigned to the proxy-holder or if there are other anomalies.

6. Supervisory Body

If any of the specified offences is committed, the Decree³⁹ prescribes the duty to oversee the functioning of and compliance with the Model and be responsible for the updating of the Model as a condition for granting exemption from the administrative responsibility entrusted to a body of the Entity (endowed with autonomous powers of initiative and control).

6.1 Identification of, appointment to and requirements for the Supervisory Body

The body must satisfy the following requirements:

▪ integrity;

For the purpose of satisfying the integrity requirements a member must not be disqualified, unfit, bankrupt or have been sentenced, including cases for which final judgement has not yet been passed, to a penalty that leads to disqualification, also temporary, from public office or the inability to exercise a managerial position, nor must a member have been convicted, including cases for which final judgement has not yet been passed, of any of the offences provided by Legislative Decree no. 231/01.

▪ autonomy and independence;

assessed with respect to the body as a whole and not its individual members, in terms of:

- the absence of conflicts of interest, also potential, with COIMA;
- the possession of autonomous powers of initiative and control;
- the lack of operational duties within COIMA;
- being in a position to report directly to the Board of Directors;

▪ professionalism understood as:

- possessing suitable specialist skills;
- having the means and specialist techniques for being able to perform the activity, including by receiving the advice of external parties;

▪ continuity understood as:

- the fact that the term of the mandate does not depend on those of other corporate bodies;
- regularity in performing controls.

Compliance with the above requirements is checked on the appointment of the body by the Board of Directors, which has named Professional Governance Overview S.r.l. as the Supervisory Body and established its relative term.

Revocation of the appointment is the responsibility of the Board of Directors and is permitted:

- i) in all cases when the law permits the termination of an employment relationship on the initiative of the employer⁴⁰;
- ii) for reasons connected with the specific failure to fulfil, whether intentionally or unintentionally, the requirements of the position (for example disloyalty, negligence, inefficiency, etc.);
- iii) in the event of impossibility;
- iv) when the requirements which members must satisfy, as stated at the preceding point, no longer hold;
- v) when the employment/collaboration relationship with COIMA ceases on the initiative of the member of the body.

If a member of the Supervisory Body is removed the Board of Directors shall arrange for his or her replacement; the member thus appointed shall remain in office until the term of the other members expires (in the case of a multi-member body).

³⁹ Article 6b.

⁴⁰ Applicable when the member of the Supervisory Body is also an employee of COIMA.

6.2 Functions and powers of the Supervisory Body

The Supervisory Body is entrusted with overseeing the following:

- application of the Model: meaning ensuring that the conduct followed within the Company corresponds to the Model;
- effectiveness of the Model: meaning ensuring that the Model is actually suitable for preventing the offences specified by the Decree and subsequent legislation that extends the field of application;
- whether it is opportune to update the Model to bring it into line with changes in the environment or in the business structure.

On a more operational level the Supervisory Body is entrusted with the duty to:

- check the map of crime risk areas (or “sensitive activities”) on a regular basis and revise this for any changes in business activities or business structure. To this end, management and persons in charge of control activities as part of the individual functions must report any situations to the Supervisory Body that may expose the Company to the risk of crime. All communications must be made in writing;
- perform checks on a regular basis, including through the use of external professionals, designed to ensure that the requirements of the Model are being complied with. In particular, ensure that the procedures and controls specified by the Model have been set up and documented as provided and that ethical principles are being followed. It should be noted, though, that control activities are devolved to the primary responsibility of operating management and are considered an integral part of every business process (“line control”), hence the importance of a personnel training process;
- check the suitability and effectiveness of the Model for preventing the crimes specified in the Decree;
- perform regular targeted checks on specific transactions or actions, especially within the area of sensitive activities. The results of these procedures must be summarized in a suitable report whose content is to be disclosed as part of communications made to the corporate bodies;
- arrange for an exchange of information with the other business functions (including by holding meetings) in order to keep crime risk/sensitive areas updated in order to:
 - keep their evolution under control to ensure constant monitoring;
 - check the various aspects relating to implementation of the Model (definition of standard clauses, personnel training, legislative and organizational changes, etc.);
 - ensure that the corrective action required to make the Model suitable and effective is performed on a timely basis;
- collect, process and store all the relevant information received in respect of the Model. To this end, the Supervisory Body has free access to all Company information that may be relevant and must be constantly informed by management about:
 - a) aspects of business activities that may expose the Company to the risk resulting from one of the crimes specified in the Decree;
 - b) relationships with Consultants and Partners;
- foster initiatives for training and communication regarding the Model and prepare the necessary documentation to that end, in conjunction with the head of training;
- interpret relevant legislation and check the adequacy of the internal control system in relation to such legislative requirements;
- report on a regular basis to the Chairman, the Board of Directors and the Board of Statutory Auditors, if appointed, on the implementation of the Company’s policies for the realization of the Model.

This structure must be capable of acting in accordance with the need to transpose, verify and implement the Models required by article 6 of the Decree, but also necessarily with respect to the need for a constant monitoring of the stage of implementation of the Models and the requirement for them to respond to the demands for prevention that the law calls for. This process of constant checking must move in two directions:

- if it emerges that the required state of implementation of the operational standards is behind, it is the duty of the Supervisory Body to adopt all the initiatives that are needed to correct this “pathological” condition. Depending on the cases and circumstances, it will therefore be a question of:
 - urging the heads of the individual organizational units to comply with the Model of conduct;
 - directly stating the corrections and changes that must be made to ordinary practices;



- reporting the more serious cases of the failure to implement the Model to the heads of the individual functions and the persons in charge of control in those functions;
- if on the other hand the need for adjustment emerges from monitoring the state of implementation, the Supervisory Body must take action to guarantee the timing and form of such adjustment⁴¹.

To this end, as stated earlier the Supervisory Body must have free access to people and all business documentation and must also have the possibility to acquire relevant data and information from the persons in charge. Finally, all the information specified below must be reported to the Supervisory Body.

The Chairman determines the role and duties of the staff dedicated wholly or partially to the Supervisory Body.

⁴¹ A timing and form that are obviously not predetermined, but the timing shall be as quickly as possible and the content shall be that required by the findings that caused the need for adjustment.

7. Information flows

7.1 Reporting by the Supervisory Body to other Corporate Bodies

The Supervisory Body has the responsibility to communicate the following to the Board of Directors:

- at the beginning of each year: a plan containing the work that it intends to perform to fulfil its assigned duties;
- on a regular basis: the state of progress of the plan and any changes made to it with the reasons for introducing these;
- immediately: any significant issues arising from its activities;
- at least annually: the extent of the implementation of the Model by COIMA.

The Supervisory Body may be called to report on its activities to the Board of Directors on a regular basis.

The Supervisory Body may additionally communicate the following, assessing the individual circumstances:

- 1) the results of its procedures to the heads of functions and/or processes, should its work give rise to aspects susceptible to improvement. In these circumstances the heads of processes must provide the Supervisory Body with an action plan, with the relative timing, for the aspects susceptible to improvement, together with the operational means required to implement the proposals;
- 2) any conduct/action not in line with the Code of Ethics and business procedures, in order to:
 - i) acquire all the information necessary to carry out any communications to the entities in charge of assessing and applying disciplinary sanctions;
 - ii) avoid repetition of the event, providing recommendations for eliminating the weaknesses.

The activities stated at point 2) must be communicated by the Supervisory Body to the Board of Directors within the shortest time possible, also by requesting support from the other business entities that may be able to assist in determining and identifying the steps that must be taken to prevent the circumstances being repeated.

Copies of the relative reports must be preserved by the Supervisory Body and by any other bodies involved from time to time.

7.2 Reporting to the Supervisory Body: general prescriptions and mandatory specific prescriptions

The Supervisory Body must be informed, by way of specific reporting by the parties bound to comply with the Model, as to any events that may give rise to the responsibility of the Company within the meaning of the Decree.

Prescriptions of a general nature

The following prescriptions of a general nature hold in this respect:

- Function directors must collect any reports on the offences contemplated by the Decree, in the event that they have been committed or where there is the reasonable risk that they will be committed, or in any case conduct in general that is not in line with the rules of behaviour established by the Model;
- employees must report any breach (or suspected breach) of the Model by contacting their direct hierarchical superior and/or the Supervisory Body (by order of the Supervisory Body “dedicated information channels” are set up to facilitate the flow of unofficial reports and information, for example telephone lines, emails or mail boxes);
- consultants, contractors and commercial partners, to the extent of the activity they perform for the Company, must report directly to the Supervisory Body through “dedicated information channels” to be determined contractually;
- the Supervisory Body assesses the reports it receives and the action that should be taken; any resulting measures are established and applied in accordance with the requirements herein concerning the disciplinary system.

People reporting in good faith are protected against any form of retaliation, discrimination or penalization, and in any case the identity of the reporting party shall be kept confidential, except for the requirements of law and the protection of the rights of the Company or those accused by mistake or in bad faith.

Mandatory specific prescriptions

In addition to the reports relating to breaches of a general nature as discussed above, information relating to the following matters must be transmitted to the Supervisory Body:

- disciplinary proceedings raised in relation to information that the Model has been breached;
- the penalties inflicted (including measures taken against employees),

or alternatively provisions to dismiss such proceedings with the relative grounds.

7.3 Reporting by Company Members or third parties

Within the Company as a whole, in addition to the documentation prescribed in the single Special Parts of the Model in accordance with the procedures contemplated therein, all other information of any nature received from third parties and relating to the implementation of the Model in the areas of activity at risk must be brought to the attention of the Supervisory Body.

The following provisions hold in this respect:

- the Supervisory Body must collect all reports regarding crimes pursuant to the Decree and committed in relation to business activities, or in any case those regarding conduct not in accordance with the lines of conduct adopted by the Company;
- all reports, including those of an unofficial nature, must be channelled to the Supervisory Body, which will assess those reports and evaluate any resulting measures at its reasonable discretion and responsibility, hearing as may be necessary the drafter of the report and/or the person responsible for the alleged violation and motivating in writing any refusal to proceed to an internal investigation;
- reporting may be in writing and have as its subject any breach or suspected breach of the Model. The Supervisory Body will act in a way to protect the reporting party against any form of retaliation, discrimination or penalization and will protect the confidentiality of the identity of the reporting party except to the extent of the requirements of law and the safeguarding of the rights of the Company or the persons accused in error or in bad faith;
- “dedicated information channels” will be set up (the “Dedicated Channel”) with a dual purpose: to facilitate the flow of reports and information to the Supervisory Body and to resolve any doubtful cases quickly.

7.4 Collection and storage of the information

All information and reports prescribed by the Model shall be stored by the Supervisory Body in a suitable electronic and/or hard copy database.

The data and information stored in the database may be made available to parties other than the Supervisory Body with the prior authorization of that Body.

The Supervisory Body shall establish the criteria and conditions for access to the database by way of a suitable provision.

8. Selection and training

8.1 Employees

Personnel selection

In conjunction with the head of personnel the Supervisory Body assesses whether to set up a specific personnel assessment system at the selection stage that takes into account requirements regarding the application of the Decree.

Employee training

For the purposes of making the Model more effective, it is the Company's objective to ensure that its head-office employees as well as its "externals" have a correct awareness of the rules of conduct contained in the Model and that these are properly disseminated. This objective regards all the staff falling into these two categories, whether the people involved are already present in the Company or have yet to enter.

The level of training and information is implemented with a different degree of depth depending on the level at which staff are involved in "sensitive activities".

Human Resources is responsible for managing personnel training for implementing the Model, in close conjunction with the Supervisory Body, and this is structured at the following levels:

- management and persons representing the Company: [initial seminar extended to all newly-hired staff at the time of employment; annual update seminar; access to hard-copy documentation and the intranet dedicated to the subject and updated by the Supervisory Body; occasional updating emails; information provided in the letter of employment for newly-hired staff];
- other personnel: internal circulars; information provided in the letter of employment for newly-hired staff; access to the internet; updating e-mails.

8.2 External Contractors and Partners

Selection of External Contractors and Partners

On the proposal of the Supervisory Body suitable assessment systems may be set up in the Company for the selection of representatives, consultants, outsourcer providers, suppliers and similar ("External Contractors") as well as Partners with which the Company intends to arrange any form of partnership (for example joint ventures, including those in the form of Temporary Associations of Companies (ATI), consortia, etc.) and which will cooperate with the Company in performing risk activities ("Partners").

Information provided to External Contractors and Partners

Information on the policies and procedures adopted on the basis of this Organizational Model may also be provided to entities outside the Company (for example Consultants and Partners) as well as the text of the contractual clauses habitually used in this respect.

9. Disciplinary system

9.1 General principles

Pursuant to article 6, paragraph 2e) and article 7, paragraph 4b) of the Decree, the Model may only be considered effectively implemented if it provides for a disciplinary system capable of sanctioning the failure to comply with its provisions.

This disciplinary system must relate to employees and senior officers and envisage suitable penalties of a disciplinary nature.

A breach by the Company's employees and/or senior officers of the rules of conduct contained in the measures prescribed by the Model constitutes non-fulfilment of the obligations deriving from the employment relationship pursuant to articles 2104 and 2106 of the Civil Code.

The application of disciplinary sanctions shall not depend on the outcome of any criminal proceedings, as the rules of conduct and internal procedures are binding for the Addressees regardless as to whether a criminal offence has actually been committed as the result of a person's behaviour.

9.2 Breach of the Model

For the purposes of compliance with Legislative Decree no. 231/01, by way of mere example any action or conduct that fails to comply with the prescriptions of the Model and/or the principles of the Code of Ethics or the failure to perform the action or conduct required by the Model while carrying out activities where there is the risk of committing one of the offences contemplated by Legislative Decree no. 231/01 shall constitute a breach of the Model.

9.3 Measures against Employees

Any conduct by employees that is in breach of the individual rules of behaviour assumed in this Model is defined as a disciplinary offence. Committing a disciplinary offence leads to the application of disciplinary sanctions.

In identifying the duty of "obedience" by the worker, article 2104 of the Civil Code requires the employee to comply with provisions of both a legal and contractual nature laid down by the employer when performing his or her work. If these provisions are not complied with, the employer may inflict disciplinary sanctions, graded on the basis of the seriousness of the infringement, in accordance with the provisions contained in the applicable National Collective Agreement.

The disciplinary system must in any case abide by the limits to sanctioning power laid down by Law no. 300 of 1970 (the "Workers' Statute"), where applicable, in terms of both the sanctions that may be inflicted and the means by which that power is exercised.

More specifically, the disciplinary system must abide by the following principles:

- a) the system must be duly made public by means of notices affixed in a place accessible to employees and if necessary must also be the subject of specific update and information courses;
- b) the sanctions must comply with the principle of proportionality with respect to the infringement, whose specifics are entrusted pursuant to article 2106 of the Civil Code to sectorial collective bargaining: in any case the choice of sanction must depend on the intentionality of the conduct or the degree of negligence, imprudence or demonstrated malpractice, on the employee's prior behaviour, with specific regard to the existence or otherwise of previous disciplinary measures, on the position of the person and the duties performed and on all other relevant circumstances, including any co-responsibility for the behaviour being sanctioned, also of an omissive nature;
- c) fines may not exceed 4 hours of basic remuneration;
- d) suspension from service and from remuneration may not exceed 10 days;
- e) workers against whom a charge is made shall be assured the right to defence (article 7 of Law no. 300/1970 and article 216 of the Civil Code): the charge shall be made on a timely basis and workers may send their written observations to the Supervisory Body within 5 working days of the charge being made and, if so requested, must also be granted the right to be heard by the Supervisory Body; in any case the

more serious disciplinary measures regarding the verbal or written reprimand cannot be applied before five working days have passed from the date of the written charge of the event that has given rise to such.

The sanction must be of a suitable level to ensure that the Model is effective.

The disciplinary sanctions are as follows:

- 1) a verbal or written reprimand, applicable if the worker breaches one of the internal procedures prescribed by the Model (for example if the worker fails to comply with the prescribed procedures, to communicate the required information to the Supervisory Body, to perform controls, etc.) or adopts behaviour in carrying out activities in the sensitive areas that fails to comply with the prescriptions of the Model;
- 2) a written caution, applicable if the worker repeatedly breaches the procedures prescribed by the Model or repeatedly adopts behaviour in carrying out activities in the sensitive areas that fails to comply with the prescriptions of the Model;
- 3) suspension from service and remuneration (not to exceed ten days), applicable if in breaching one of the internal procedures specified by the Model or in carrying out activities in the sensitive areas the worker adopts behaviour that fails to comply with the prescriptions of the Model, causes damage or creates a situation of potential risk for the Company, or if the worker has repeatedly committed the violation referred to in paragraph 2;
- 4) the termination of the employment relationship for just cause, applicable if the worker adopts behaviour in carrying out activities in the sensitive areas that fails to comply with the prescriptions of the Model and constitutes significant non-fulfilment, unequivocally directed towards committing a crime sanctioned by Legislative Decree no. 231/01 or which causes the actual application of the measures prescribed by Legislative Decree no. 231/01 against the Company;
- 5) the termination of the employment relationship for just cause, applicable if in carrying out activities in the sensitive areas the worker engages in conduct that fails to comply with the prescriptions of the Model and constitutes significant non-fulfilment, aimed unequivocally at committing a crime sanctioned by Legislative Decree no. 231/01 or which causes the actual application of the measures specified in Legislative Decree no. 231/01 against the Company, or who has repeatedly committed the violation referred to in paragraph 3.

It is understood that all the provisions and guarantees provided by the law and employment contracts on disciplinary provisions shall be followed; in particular the following shall be complied with:

- the requirement – in relation to the application of any disciplinary provision – for the charge to have been previously been raised against the employee and for the employee's defence to be heard;
- the requirement, with the sole exception of a verbal caution, that the charge be made in writing and that the provision shall not be issued until the number of days specifically stated for each sanction in the employment contracts has passed since the charge was raised.

As regards the establishment of infringements, the disciplinary proceedings and the infliction of sanctions, the powers granted to the Company's management remain valid within the limits of the respective powers and responsibilities.

The type and extent of each of the above sanctions shall be applied also considering:

- the intentional nature of the behaviour and the degree of negligence, imprudence or malpractice also with regard to the predictability of the event;
- the overall conduct of the worker, with particular regard to the existence of disciplinary antecedents, within the limits permitted by the law;
- the worker's duties;
- the functional position and level of responsibility and autonomy of those involved in the facts constituting the breach;
- any other special circumstances surrounding the disciplinary offence.

9.4 Measures against Directors

If one or more members of the Board of Directors breaches current legislation or fails to comply with the internal procedures specified by the Model or by the Code of Ethics, the Supervisory Body shall inform the whole Board of Directors and the Board of Statutory Auditors, which, with the exclusion of the director concerned, shall take suitable measures pursuant to current legislation.



If the sanctionable conduct pursuant to and in accordance with this Model is engaged by the majority of members of the Board of Directors, the Supervisory Body shall inform the Board of Directors and the Board of Statutory Auditors. The Board of Directors shall call a shareholders' meeting in order to adopt the most suitable measures, and if not, this shall be called by the Board of Statutory Auditors.

The director and/or directors who are charged with violating the prescriptions of the Model are entitled to submit their defence on a timely basis before the above measures are taken.

9.5 Measures against Senior Officials

If senior officials violate current law or fail to comply with the internal procedures specified by the Model or by the Code of Ethics, the most appropriate measures will be applied against them in accordance with current legislation and the respective National Collective Labour Agreement for Executives.

9.6 Measures against Contractors, Consultants and other third parties

Any conduct by contractors, consultants, suppliers, partners or other third parties who are linked to the Company by a contractual relationship that is not an employment relationship, which violates the prescriptions of the Model and/or the Code of Ethics, may, in accordance with the specific contractual clauses included in the engagement letter or also in their absence, lead to the termination of the contractual relationship, without prejudice to any possible claim for damages if such conduct causes harm to the Company, regardless of the termination or not of the contractual relationship.