ITALIAN CERAMIC SURFACES

# ORGANISATION, MANAGEMENT AND CONTROL MODEL

# SICER S.P.A.

# pursuant to Italian Legislative Decree no. 231 of 8 June 2001 and subsequent amendments and integrations

**approved for the first time by the Board of Directors on 15/09/2017**

ITALIAN CERAMIC SURFACES

## CONTENTS

## General Section

ITALIAN CERAMIC SURFACES

## Special Section

Special Section A – Code of ethics
Special Section B – Organisational structure
Special Section C – System of delegation and powers
Special Section D – Penalty system
Special Section E – Offences committed against the Public Administration or to the detriment of the State
Special Section F – Offences of counterfeiting money, credit cards, stamps and identity instruments or signs
Special Section G – Corporate offences
Special Section H – Crimes against the individual
Special Section I – Offences relating to safety in the workplace
Special Section J – Offences relating to receiving stolen goods, money laundering, the use of money, goods or benefits that are the proceeds of crime, and self-laundering
Special Section K – Transnational offences under law of 16 March 2006 no. 146
Special Section L – Offences relating to cybercrime and unlawful data processing
Special Section M – Breach of copyright offences
Special Section N – Crimes against industry and trade
Special Section O – Crime referred to in art. 377-*bis* Italian Criminal Code
Special Section P – Structure, composition, regulation and functioning of the Supervisory Body
Special Section Q – Organised crime
Special Section R – Offence of employing illegally staying third country nationals
Special Section S – Environmental offences
Special Section T – Internal company regulations for the management of staff and company assets
Penalties handbook

# 1. ITALIAN LEGISLATIVE DECREE OF 8 JUNE 2001, NO. 231

Italian Legislative Decree of 8 June 2001 no. 231 setting out the "Regulation of administrative responsibilities of legal persons, companies and associations, even without legal personality, pursuant to article 11 of law no. 300 of 29 September 2000", (in short: the "Decree"), which entered into force on 4 July 2001, is understood to adapt Italian legislation, regarding the liability of legal persons, to the international conventions to which Italy has been party for some time, in particular:

- the Brussels Convention of 26 July 1995 on the protection of the European Community's financial interests,
- the Brussels Convention of 26 May 1997 on the fight against corruption involving officials of the European Communities or officials of member states of the European Union,
- the OECD Convention of 17 December 1997 on Combating Bribery of Foreign Public Officials in International Business Transactions.

This Decree introduced into Italian law, for legal persons (in short: "companies") a system for administrative responsibility – which is in fact comparable to criminal liability ([1]) which expands on the liability of the natural person who materially committed certain unlawful acts, and which seeks to include, in punishing that person, the companies in whose interest or benefit the offences in question have been committed.

The liability provided for in the Decree also applies to offences committed abroad, provided that no legal proceedings have been taken by the State where the offence was committed.

The entity shall be liable even if the offender has not been identified, and shall remain liable even if the offence itself is extinguished with respect to the offender for any reason other than amnesty or a limitation period.

The administrative penalties applied to the entity shall be time-barred for proceedings, unless the limitation period is interrupted, for a period of 5 years from the date the offence is committed.

## 1.1. Principle of legality

The entity is liable within the limitations established by the law: the entity "cannot be held liable for an act that constitutes an offence, if its [criminal] liability with respect to that offence and related penalties are not expressly established by a law which was in force before such act took place" (article 2 of the Decree).

## 1.2. Objective criteria for the allocation of liability

There are three types of objective criteria for the allocation of liability:

a) The committing of one of the offences set out in the Decree from art. 24 to art. 25-*duodecies*.
b) The offence must have been committed "in the interests or to the advantage of the entity".

***Interest and/or advantage***

Another element of the liability in question is the need for the supposed unlawful conduct to be performed in the interest or to the advantage of the Entity.

The interest or advantage of the Entity is considered on the basis of the liability of the latter, even in cases where there are also interests or advantages for the party committing the offence or for third parties, with the only limit being the hypothesis in which the offence being committed by an individual in a qualified position within the Entity, lies exclusively with the offender or with third parties.

([1]) The "criminal" nature of this liability has four elements: 1) it derives from the offence in the sense that the offence constitutes a prerequisite for the penalty; 2) it is confirmed with the guarantees of the criminal process and by a criminal judge; 3) it involves the application of penalties (financial penalties and restrictive penalties); 4) negligence plays a central role, under the principle of guilt.

Since no exempting effect has been acknowledged to the exclusive "advantage" of the offender or third parties, but only - as stated - in the sole interests of these individuals, the Entity should be held liable even if it does not gain any advantage or when there is an exclusive benefit for the offender or a third party, provided that the Entity has an interest, possibly competing with that of a third party, in the offence being committed by qualified persons in its organisation.
Moving beyond the aforementioned specifications, the liability provided for by the Decree therefore arises not only when the unlawful behaviour has determined an advantage for the Entity itself, but also in the hypothesis that, even in the absence of such a concrete outcome, the unlawful act is justified in the interests of the Entity. The two wordings express legally different concepts and represent alternative assumptions, each with its own autonomy and scope of application.
Regarding the terms "interest" and "advantage", the government report accompanying the Decree gives the first a decidedly subjective value, susceptible to an *ex ante* valuation (known as benefit-focused) and the second a decidedly objective value (referring to the actual outcome of the conduct of the acting party which, even if it was not directly focused on the entity's interest, has created, with its conduct, an advantage in its favour) susceptible to *ex post* verification.
The essential features of interest are identified as: objectivity, understood as independence from the personal, psychological beliefs of the agent and, correspondingly, a necessary basis in external elements susceptible to verification by any observers; concreteness, understood as registration of the interest not merely in hypothetical and abstract terms, but in real terms, to safeguard the principle of harm; currency, in the sense that the interest must objectively exist and be recognisable in the moment when the act is acknowledged and must not be future or uncertain, otherwise it lacks the damage for classification as an offence rather than a simple danger; not necessarily financial significance, but traceability to company policy.
In terms of content, the advantage traceable to the Entity – which must be kept separate to profit – can be: direct, i.e. traceable exclusively and directly to the Entity; indirect, i.e. mediated by results acquired by third parties, which could still have positive repercussions for the Entity; financial, even if not necessarily immediate.

***"Group" interest***

The Court of Cassation (Sec. V, 17 November 2010 - 18 January 2011, public prosecutor, Court of Bari in the case of Tosinvest Servizi s.r.l. et al) for the first time addressed the issue of criteria for the allocation of administrative liability governed by Legislative Decree no. 231 of 2001 within a *holding* or other companies that are part of a group that includes one or more structures directly attributed with the aforementioned liability by virtue of criminal conduct carried out by persons holding a qualified position within the meaning of art. 5 paragraph 1.
Judgements on the merits that had previously been made on a level completely ignored by the regulatory system in force, despite the spread of the phenomenon of corporate groups in modern economic reality, had already partially marked, albeit with different accents, the guidelines for the extension of administrative liability to the various components of a business combination.
An initial limit to the expansive approach of the aforementioned liability was identified in the subjective criteria for allocation postulated by the Decree, according to which there must be a qualified relationship between the entity (whether this is a holding, parent company or subsidiary) whose position is being discussed and the perpetrator of the presumed offence who must hold, within that entity, an executive or subordinate role with respect to the parties exercising the prerogatives of management or supervision (Court of Milan, 20 December 2004, in *www.rivista231.it*; Court of Milan, 14 December 2004, Cogefi, in *Foro It.*, 2005, II, 527).
The last factor in extending liability was then identified as what is known as "group interest", evoked from time to time in the scale attributed to the same by the Civil Code, following the reform of corporate law and civil case law (Court of Milan, 20 September 2004, Ivri Holding et al, in *Foro It.*, 2005, 556), on other occasions moving away from the criteria for allocation set out within the Decree (in particular in art. 5 par. 2 - 12 par. 1 a) - 13 final

paragraph) read in light of the significant link between the various entities involved (Preliminary investigations judge, Court of Milan, 26 February 2007, Fondazione M. et al, in *La responsabilità amministrativa delle società e degli enti* [The administrative liability of companies and entities], 2007, 4, 139). From the perspective outlined above, since the entity is not liable only if the offender has acted exclusively in its own interest or the interest of a third party, it is deemed to exclude, since the conditions of the subsidiary inevitably have repercussions for the parent company, both that the advantages obtained by the subsidiary, as a result of the parent company's activity, can be deemed to have been gained by a third party, and that the activity of the subsidiary can be regarded as being in the sole interest of a third party (Court of Milan, 20 December 2004, cit.). Definitively, the liability of the legal person within which a qualified position is held by the perpetrator of the offence committed in the interest or to the advantage of other members of the same business combination, unfailingly postulates the acknowledgement of links or ties between the entities in question that do not allow the entity favoured to qualify as a third party, which means that, upstream, the offence committed can objectively be seen as intended to satisfy the interest of several parties, including the legal person that employs the party responsible for the offending conduct. (EPIDENDIO, sub *Art. 5 Decree Law 8 June 2001, no. 231*, cit., 9458).
In the matter submitted for examination by the Supreme Court, the local court, at a preliminary hearing, found that some members of the group of companies related to the perpetrator of the corrupt conduct under dispute did gain an advantage from that conduct, while other companies, even though they could be attributed to the same financial group, would not have gained any significant benefit, meaning that no charge could be brought against them under the Decree.
In view of an appeal aimed at highlighting, in the opposite sense, the fact that the physical person in an executive position charged with corruption was also the de facto director of companies which were deemed not to be involved, the Supreme Court Judges state the three conditions which must necessarily be met for an entity's liability to be asserted, that is, the perpetration of one of the liable offences provided for by the Decree, the offence being committed by a party that has an organisational/functional link to the legal person, and finally the pursuit of an interest or the acquisition of an advantage for the entity, both to be verified in practice.
With particular reference to the holding and group companies other than the one on whose behalf the alleged offender has acted, the second of the three conditions outlined can be considered to be met whenever the party acting on behalf of the same is in competition with the natural person who has committed the alleged offence; in that sense, this is not a generic reference i.e. the entity's membership of the same group that includes the party directly attributed with administrative liability.
With regard to the further assumption of interest or advantage, the holding or other group company can be held liable under the provisions of the Decree only where they achieve potential or real usefulness, albeit not necessarily of a financial nature, deriving from the alleged crime, which is, however, still to be confirmed.
Ultimately, the Supreme Court Judge seems to endorse the argument that the interest of the entity (parent company, controlling company or subsidiary company) in the consummation of the alleged offence cannot arise from the existence of another interest of the group to which that entity belongs, but rather from the specific recognition of the interest pursued by the consummation of the offence and the verification of its traceability also to the legal person in question, in the light of the links, in fact or in law, existing with the various elements of business combination and, in particular, with the one to which the principal perpetrator of the offending conduct belongs.

***Interest and/or advantage in negligent offences***

The legislation on the criminal liability of entities is generally based on alleged offences of an intentional nature.
The introduction of negligent offences with regard to safety in the workplace – starting with the law of 3 August 2007, no. 123 ("new" art. 25-*septies* later repealed and replaced by art. 300 legislative decree of 9 April 2008, no. 81) – again raised the absolutely central nature of the issue of the subjective matrix of criteria for allocation.

From this point of view, while, on the one hand, it is claimed that in negligent offences the pairing of the concepts of interest and advantage must refer not to the unintended unlawful events, but to the conduct of the natural person in performing their activity, on the other hand, it is maintained that negligent offences, from a structural point of view, cannot be reconciled with the concept of interest.
It follows, therefore, that in this context, insofar as it is possible to hypothesise how the omission of the proper behaviour imposed by rules of a precautionary nature – intended to prevent accidents in the workplace – could translate into controlling company costs, which could be qualified *ex post* as an "advantage" (if we think, for example of the failure to supply protective equipment, or the failure to review any type of equipment dictated by savings requirements).

The criminal offence must have been committed by one or more qualified parties, or "by persons who hold representative, administrative or managerial roles for the company or one of its organisational units which has financial and operational autonomy", or by parties who "perform, even de facto, the management and control" of the entity (parties in so-called "executive positions"); or even "by persons subject to the management or supervision of an executive party" (so-called "subordinates").
The perpetrators of an offence that could incur the entity's administrative liability may therefore be: 1) parties in "executive positions" such as, for example, a legal representative, director, CEO, or site manager, and the persons who perform, even de facto, the management and control of the entity; 2) "subordinate" individuals, typically dependent workers, but also parties from outside the entity, who have been entrusted with task to perform under the management and supervision of executives.
If several individuals are involved in committing the offence (hypothesis for collusion in the offence *ex* art. 110 of the Criminal Code), the "qualified" party does not need to take the usual action provided for by criminal law. It is sufficient for them to make a knowingly causal contribution to the offence being committed.

## 1.3. Subjective criteria for the allocation of liability

The subjective criteria for the allocation of liability are put into effect when the offence demonstrates a connotative approach in company policy or at least depends on negligence in the organisation.
The provisions of the Decree exclude the entity's liability where the entity – before the offence was committed – has adopted and effectively implemented a suitable "model for organisation and management" (shortened to: "model") to prevent the committing of offences of the nature of the offence that has been committed.
The entity's liability in this regard is traced back to the "failure to adopt or failure to comply with due standards" relating to organisation and activities within the entity; this fault can traced back to company policy or to structural and prescriptive failings in company organisation.

## 1.4. Type of offences considered

The operational scope of the Decree concerns the following offences:

- *Offences committed against the Public Administration or to the detriment of the State (article 24 and 25 of the Decree)*

Embezzlement to the detriment of the State (art. 316-*bis* of the Italian Criminal Code);
Misappropriation of public disbursements to the detriment of the State (art. 316-*ter* of the Italian Criminal Code);
Fraud to the detriment of the State or another public body or with the aim of exempting someone from military service (art. 640, paragraph 2, no. 1, of the Italian Criminal Code);
Aggravated fraud for the obtainment of public disbursements (art. 640-*bis* of the Italian Criminal Code);
Computer fraud (art. 640-*ter* of the Italian Criminal Code);

Corruption for an official act (art. 321 of the Italian Criminal code);
Corruption for the exercise of a function (art. 318 Italian Criminal code);
Incitement to corruption (art. 322 of the Italian Criminal Code);
Extortion (art. 317 of the Italian Criminal Code);
Corruption for an act not compliant with official duties (art. 319, 319-*bis* and 321 of the Italian Criminal Code);
Corruption in judicial acts (art. 319-*ter*, paragraph 2 and 321 of the Italian Criminal Code);
Unlawful incitement to give or promise benefits (art. 319-*quater*);
Corruption of a public officer (article 320 of the Italian Criminal Code);
Embezzlement, misappropriation of office, corruption and incitement to corruption of members of bodies of the EU and officials of the EU and foreign states (art. 322-*bis* of the Italian Criminal Code).

- by virtue of the promulgation and entry into force of decree law 25 September 2001 no. 350 converted with amendments to law 23 November 2001 no. 409 and by virtue of the additions made to the promulgation and entry into force of law no. 99 of 2009, *the offences set out in art. 25 bis of the Decree, i.e. offences of counterfeiting money, credit cards, stamps and identity instruments or signs:*

Counterfeiting of coins/money, spending and introduction into the State, acting in concert, of counterfeit money (article 453 of the Italian Criminal Code);
Modification of money (article 454 of the Italian Criminal Code);
Spending and introduction into the State of counterfeit money, not acting in concert, (article 455 of the Italian Criminal Code);
Spending of counterfeit money/coins received in good faith (art. 457 of the Italian Criminal Code);
Forgery of stamps, introduction thereof into the State, purchase, holding or circulation of counterfeit stamps (art. 459 of the Italian Criminal Code);
Forging/counterfeiting of watermarked paper used to make credit cards or stamp duties (art. 460 of the Italian Criminal Code);
Fabrication and holding of watermarks or instruments used to counterfeit money, stamp duties or watermarked paper (art. 461 of the Italian Criminal Code);
Use of counterfeit or modified stamps (art. 464 of the Italian Criminal Code)
Counterfeiting, modifying or using trademarks or distinctive signs, i.e. patents, models and designs (article 473 of the Italian Criminal Code)
Introducing and trading in the State of products with false signs (art. 474 of the Italian Criminal Code).

- by virtue of the promulgation and entry into force of the Italian legislative decree of 11 April 2002 no. 61 as amended by law 28 December 2005 no. 262 and by virtue of the amendments made to the promulgation of law 27 May 2015, no. 69 and of Italian Legislative Decree 38/2017 *the offences set out in art. 25*-ter *of the Decree, i.e. corporate offences:*

- False corporate disclosures (art. 2621 Italian Civil Code);
Minor offences (art. 2621-*bis* Italian Civil Code);
False corporate disclosures in listed companies (art. 2622 Italian Civil Code);
False reporting in prospectuses (art. 2623 Italian Civil Code – art. 173-*bis* law 24 February 1998 no. 58)
False reporting or communication by an auditing firm (art. 2624 Italian Civil Code – abrogated by art. 37 par. 34 Italian Legislative Decree no. 39/2010 and replaced by art. 27 of the same decree entitled: “False reporting or communication by those responsible for legal auditing“;
Obstruction of supervisory activities (article 2625 Italian Civil Code, par. 1 as amended by art. 37, par. 35 of Italian Legislative Decree no. 39/2010 and referenced by art. 29 of the same decree);
Unlawful restitution of shareholders’ contributions (art. 2626 Italian Civil Code);

Illegal distribution of profits and reserves (article 2627 Italian Civil Code);
Illegal operations involving the shares or quotas of the company or parent company (article 2628 Italian Civil Code);
Transactions to the detriment of creditors (article 2629 Italian Civil Code);
Fictitious formation of share capital (article 2632 Italian Civil Code);
Unlawful allocation of company assets by liquidators (article 2633 Italian Civil Code);
Bribery between private individuals (art. 2635 Italian Civil Code);
Instigating bribery between private individuals (art. 2635-*bis* Italian Civil Code)
Unlawful influence on shareholders' meetings (article 2636 Italian Civil Code);
Stock fraud (article 2637 Italian Civil Code);
Hindering the activity of state supervisory authorities (article 2638 Italian Civil Code).

- following the promulgation and entry into force of law 14 January 2003 no. 7, *the offences set out in art. 25-*quater *of the Decree, i.e. what are known as offences for the purposes of terrorism or the subversion of democratic order provided for by the criminal code and by special laws.*

- by virtue of the promulgation and entry into force of law 9 January 2006 no. 7, *the offences set out in art. 25-*quater*.1 of the Decree, i.e. what are known as offences of the practice of female genital mutilation.*

- by virtue of the promulgation and entry into force of law 11 August 2003 no. 228 as amended by law 6 February 2006 no. 38 and by Italian Legislative Decree 4 March 2014, no. 39 and by Law no. 199/2016, *the offences set out in art.* 25-quinquies *of the Decree i.e. crimes against the individual governed by section I chapter III volume XII of book II of the criminal code.*

- following the promulgation and entry into force of law 18 April 2005 no. 62, *the offences set out in art. 25-*sexies *of the Decree, i.e., the offences provided for by part V, section I bis, chapter II of the consolidated act referred to by Italian Legislative Decree 24 February 1998 no. 58, offences relating to market abuse:*
misuse of privileged information (art. 184 Italian Legislative Decree 24 February 1998, no. 58);
market manipulation (art. 185 Italian Legislative Decree 24 February 1998, no 58).

- following the promulgation and entry into force of the law on "Ratification and Enforcement of the United Nations Convention and Protocols against Transnational Organised Crime adopted by the General Assembly on 15 November 2000 and 31 May 2001", finally approved and published in Official Bulletin of 11 April 2006, *transnational offences under the scope of law 16 March 2006 no. 146*, i.e. the offences of:

Criminal conspiracy (article 416 Italian Criminal Code);
Mafia organisation (article 416-*bis* Italian Criminal Code);
Criminal conspiracy for the smuggling of foreign tobacco products (article 291-*quater* Presidential Decree 23 January 1973 no. 43);
Associating for the illegal trade of drugs and psychotropic substances (art. 74 Presidential Decree 9 October 1990 no. 309);
Money laundering (art. 648-*bis* Italian Criminal Code);
Use of money, goods or benefits that are the proceeds of crime (art. 648 *ter* Italian Criminal Code);
Offences relating to the trafficking of migrants provided for by art. 12 par. 3, 3-*bis*, 3-*ter* and 5 Italian Legislative Decree 25 July 1998 no. 286;
Obstruction against justice: inducing to not make statements or making false statements to the legal authorities (article 377-*bis* Italian Criminal Code);
Obstruction against justice: abetting (art. 378 Italian Criminal Code).

- following the promulgation and entry into force of law 3 August 2007 no. 123, the offences provided for by art. 25-septies *committed in breach of regulations on accident prevention and health and safety in the workplace,* or the crimes of:

  Involuntary manslaughter in breach of regulations on accident prevention and health and safety in the workplace (art. 589 Italian Criminal Code);

  Serious and very serious personal injury through negligence in breach of regulations on accident prevention and health and safety in the workplace (art. 590 Italian Criminal Code).

- following the promulgation and entry into force of Italian Legislative Decree 21 November 2007 no. 231 and by virtue of the amendments made by law 15 December 2014 no. 186, *the offences provided for by art. 25*-octies *(Receiving stolen goods, money laundering, the use of money, goods or benefits that are the proceeds of crime, and self-laundering)*, i.e. the crimes of:

  Receiving stolen goods (art. 648 Italian Criminal Code);

  Money laundering, (art. 648-*bis* Italian Criminal Code);

  The use of money, goods or benefits that are the proceeds of crime (art. 648-*ter* Italian Criminal Code).

  Self-laundering (art. 648-*ter.* 1 Italian Criminal Code)

- following the promulgation and entry into force of law 18 March 2008 no. 48, *the offences provided for by art. 24 bis*, i,e, cybercrimes and unlawful data processing:

  Unauthorised access to a computer or ICT system (art. 615-*ter* Italian Criminal Code);

  Intercepting, preventing or illicitly interrupting computer or ICT communications (art. 617-*quater* Italian Criminal Code);

  Installation of devices to intercept, prevent or interrupt computer or ICT communications (art. 617-*quinquies* Italian Criminal Code);

  Damage to computer or ICT systems (art. 635-*bis* Italian Criminal Code);

  Damage to computer or ICT systems used by the State, by another public entity or otherwise for public use (art. 635-*ter* Italian Criminal Code);

  Damage to computer or ICT systems (art. 635-*quarter* Italian Criminal Code);

  Damage to public computer or ICT systems (art. 635-*quinquies* Italian Criminal Code);

  Electronic documents (art. 491-*bis* Italian Criminal Code);

  Computer fraud by the subject providing electronic signature certification services (art. 640-*quinquies* Italian Criminal Code).

- following the promulgation and entry into force of law no. 94 of 2009, *the offences provided for under art.* 24-ter, i.e. organised crime:

  Criminal conspiracy (art. 416 Italian Criminal Code);

  Criminal conspiracy to commit one of the offences under art. 600, 601 and 602 Italian Criminal Code (art. 416 par. 6 Italian Criminal Code);

  Mafia organisation (article 416-*bis* Italian Criminal Code);

  Electoral intrigue with mafia-like associations (art. 416-*ter* Italian Criminal Code);

  Kidnapping for ransom (art. 630 Italian Criminal Code);

  Associating for the illegal trade of drugs and psychotropic substances (art. 74 Presidential Decree 9 October 1990 no. 309).

- following the promulgation and entry into force of law no. 99 of 2009, *the offences provided for under art. 25*-bis.*1,* i.e. crimes against industry and trade:

  Disturbed freedom of industry and trade (art. 513 Italian Criminal Code);

Unlawful competition with threat or violence (art. 513-*bis* Italian Criminal Code);
Fraud against national industries (art. 514 Italian Criminal Code);
Fraud in trade (art. 515 Italian Criminal Code);
Sale of non-genuine foods as genuine (art. 516 Italian Criminal Code);
Sale of industrial products under false marks (art. 517 Italian Criminal Code);
Production and trade of goods made by encroaching on industrial property rights (art. 517-*ter* Italian Criminal Code);
Counterfeiting geographical indications or denominations of origin of agricultural food products (art. 517-*quater* Italian Criminal Code).

- following the promulgation and entry into force of law no. 99 of 2009, *the offences provided for under art. 25*-novies, i.e. breach of copyright offences

Art. 171 par. 1a *bis* and 3 law 22 April 1941 no. 633, Protection of copyright and other rights related to exercising copyright;
Art. 171-*bis* law 22 April 1941 no. 633;
Art. 171-*ter* law 22 April 1941 no. 633;
Art. 171-*septies* law 22 April 1941 no. 633;
Art. 171-*octies* law 22 April 1941 no. 633.

- following the promulgation and of law 3 August 2009 no. 116, *the offence provided for under arts. 25*-decies, i.e. the Office of incitement not to report or to make false reports to the legal authorities (art. 377-*bis* Italian Criminal Code), at national level.

- Following the promulgation of Italian Legislative Decree 7 July 2011 no. 121 and by virtue of the amendments made by law 22 May 2015, no. 68, *the offences provided for by art. 25*-undecies, i.e. environmental offences:

Environmental pollution (art. 452-*bis* Italian Criminal Code);
Environmental disaster (art. 452-*quater* Italian Criminal Code);
Negligent crimes against the environment (art. 452-*quinquies* Italian Criminal Code);
Trafficking and abandonment of highly radioactive material (art. 452-*sexies* Italian Criminal Code);
Killing, destruction, capture, collection, detention of specimens of protected species of wild animals or plants (art. 727-*bis* Italian Criminal Code);
Destruction or deterioration of habitats within a protected site (art. 733-*bis* Italian Criminal Code);
Arts. 137, 256, 257, 258, 259, 260, 260 *bis* and 279 Italian Legislative Decree 3 April 2006 no. 152, environmental standards;
Arts. 1, 2 and 3 *bis* law 7 February 1992 no. 150, Discipline of offences relating to the application in Italy of the Convention on International Trade in Endangered Animal and Vegetable Products, signed in Washington on March 3, 1973, set out in law 19 December 1975 no. 874, and regulation (EEC) no. 3626/82, and subsequent amendments, as well as rules for the marketing and possession of live specimens of mammals and reptiles which may pose a risk to public health and safety;
Art. 3 law 28 December 1993 no. 549, Measures to protect the ozone layer and the environment;
Arts. 8 and 9, Italian Legislative Decree 6 November 2007 no. 202, Implementation of Directive 2005/35/EC on pollution caused by ships and consequent sanctions.

- following the promulgation of Italian Legislative Decree 16 July 2012 no. 109, *the offence provided for by art. 25*-duodecies, i.e. the offence of employing illegally staying third-country nationals (art. 22 par. 12-*bis* Italian Legislative Decree 25 July 1998 no. 286).

## 1.5. Offences committed abroad

Pursuant to art. 4 of the Decree, the entity may be called to answer charges in Italy in relation to certain offences committed abroad.
The conditions for this liability are:

a) the offence must be committed abroad by a party with a working relationship with the company;
b) the company must have its registered office in the territory of the Italian State;
c) the company can be held liable only in the cases and under the conditions set out in arts. 7, 8, 9 and 10 Italian Criminal Code and if the law provides that the guilty party – a natural person – should be punished at the request of the Ministry of Justice, action will be taken against the company only if the request is also made to the latter;
d) where the cases and conditions set out in the aforementioned articles of the criminal code are in place, the company can be held liable provided that no action is being taken against it by the State in which the offence was committed.

## 1.6. Penalties

The administrative penalties for administrative violations resulting from offences are:

- financial penalties;
- restrictive penalties;
- confiscation of property;
- publication of judgement.

Financial penalties shall always apply to administrative violations resulting from offences. The judge determines the financial penalty taking into account the severity of the act, the degree of the Company's liability, and the steps taken by the latter to eliminate or reduce the consequences of the act or to prevent further violations from being committed.

The financial penalty is reduced when:

- the offender has committed the offence mainly in his/her own interest or the interest of third parties and the company has not gained any advantage from the offence, or when this advantage is minimal;
- the related damage is particularly insignificant;
- the company has fully paid compensation for the damage and has eliminated the damaging or dangerous consequences of the offence, or it has endeavoured to do so;
- the company has adopted and implemented a suitable organisational model to prevent other similar offences being committed.

Restrictive penalties apply when at least one of the following conditions is met:

- the company has obtained a significant profit from the offence – committed by one of its employees or by a person in an executive position – and the committing of the offence was determined or facilitated by serious organisational failings;
- where the unlawful acts have been performed more than once.

In particular, the main restrictive penalties are:

- prevention from performing activities;
- suspension or cancellation of the authorisations, licenses or concessions used to commit the offence;
- a ban from entering into contracts with the public administration, except in the case of using a public service;

- exclusion from benefits, financing, grants or subsidies and the cancellation of any already granted;
- a temporary or permanent ban on advertising goods or services.

Where necessary, multiple restrictive penalties can be applied.

With regard to the entity, there is the possibility, upon sentencing, for the confiscation of the price or profit of the offence, except for any part that can be returned to the injured party. Rights acquired by third parties in good faith are preserved.
Confiscation can also be implemented for an “equivalent”, i.e. where confiscation cannot be ordered for the price or profit of the offence, it may be ordered for sums of money, property or other assets with a value equivalent to the price or profit of the offence.

The publication of the sentence may be ordered when a restrictive penalty is applied against the Company.

If the requirements are met for the application of a restrictive penalty that determines the interruption of the company’s activities, the judge, instead of applying the penalty shall order the continuation of the company’s activity by a receiver for a period equal to the duration of the restrictive penalty to be applied, when at least one of the following conditions is met: a) the company performs a service required by the public, the interruption of which could cause serious harm to the community; b) the interruption of the company’s activity could, considering its size and the financial conditions of the territory in which it is located, have a serious effect on employment.
Profits derived from the continuation of activity will be confiscated.

Restrictive penalties can also be applied with permanent effect.
A permanent ban on performing the activity can be ordered if the company made a significant profit from the offence and has already received, at least three times within the last seven years, a temporary ban from performing its activity.

The judge can apply a permanent ban preventing the company from entering into contracts with the Public administration, or advertising goods or services when the company has already been issued with the same penalty at least three times within the last seven years.

If the company, or one of its organisational units, is regularly used for the sole or main purpose of enabling or facilitating the committing of offences in relation to which there are provisions for its liability, it shall always be issued with a permanent ban from performing its activities.

Also significant in this context is art. 23 of the Decree, which makes provisions for the offence of “Failure to comply with restrictive penalties”.

This offence is committed when, in performing the activities of the Entity that has been issued with a restrictive penalty, the obligations or bans set out in those penalties are breached.

Furthermore, if by committing the aforementioned offence, the Entity makes a significant profit, there are provisions for the application of different restrictive penalties in addition to those already imposed.

By way of example, the offence may be committed in the case where the Company participates in a public tender regardless of the fact that it is subject to a restrictive penalty preventing it from entering into contracts with the Public administration.

## 1.7. Real and precautionary restrictive measures

A restrictive penalty may be applied to the company as a precautionary measure, or a seizure or attachment may be ordered.

A precautionary restrictive measure – which consists of the temporary application of a restrictive penalty – is ordered when two requirements are met: a) when there are serious indications that the company is liable for an administrative violation resulting from offences (serious indications exist in the event of one of the conditions set out art. 13 of Decree: the company has obtained a significant profit from the offence – committed by one of its employees or by a person in an executive position – and the committing of the offence was determined or facilitated by serious organisational failings; where the unlawful acts have been performed more than once; b) where there is well-founded and specific evidence that implies a real danger of further similar offences being committed.

Real precautionary measures take the form of a seizure or attachment.
A seizure is ordered for the price or profit of the offence, where the offence can be attributed to the company, no matter whether there are serious indications of the guilt of the company itself.

An attachment is ordered for the company's moveable or immoveable property and for sums or things owed to the company, if there are well-founded grounds to believe that the guarantees for the payment of the financial penalty, procedural costs or any other sum owed to the State treasury may not exist or be lost.

Also important in this context is art. 23 of the Decree, which makes provisions for the offence of "Failure to comply with restrictive penalties".

This offence is committed when, in performing the activities of the Entity that has been issued with a restrictive penalty, the obligations or bans set out in those penalties are breached.

Furthermore, if by committing the aforementioned offence, the Entity makes a significant profit, there are provisions for the application of different restrictive penalties in addition to those already imposed.

By way of example, the offence may be committed in the case where the Company participates in a public tender regardless of the fact that it is subject to a restrictive penalty preventing it from entering into contracts with the Public administration.

## 1.8. Actions exempt from administrative liability

Art. 6 par. 1 of the Decree provides for a specific form of exemption from administrative liability when the offence is committed by individuals in so-called "executive positions" and the Company proves that:
the management body adopted and effectively implemented, before the unlawful act was committed, a suitable model to prevent other similar offences being committed;
it has entrusted to an internal body, known as the supervisory body – granted autonomous powers of initiative and control – the task of supervising the operation and effective compliance with the model in question and to ensure that it is kept up to date;

the individuals in so-called “executive positions” committed the offence by fraudulently circumventing the model; there has been no lack of control or insufficient control by the so-called Supervisory Body.

Art. 6 par. 2 of the Decree also provides that the model should meet the following requirements:

- identify corporate risks, i.e. the activities within which offences can be committed;
- exclude the possibility that any person working within the Company could justify their own conduct by claiming ignorance of the company regulations and avoid the possibility that, under normal circumstances, the offence could be caused by an error – including errors due to negligence or inexperience – in evaluating the company regulations;
- introduce a disciplinary system with the related penalties for non-compliance with the model's measures;
- identify methods to manage financial resources and prevent such offences from being committed;
- establish a system of preventive controls that can only be circumvented intentionally;
- establish information obligations with regard to the Supervisory Body appointed to monitor the functioning of and compliance with the models;

Art. 7 of the Decree provides for a specific form of exemption from administrative liability when the offence is committed by so-called “subordinate” individuals but it is ascertained that the Company, before the offence was committed, had adopted a suitable model to prevent other similar offences being committed.

Specifically, to be exempt from administrative liability, the Company must:

- adopt a Code of Ethics that sets out principles of conduct in relation to the offence;
- establish an organisational structure capable of ensuring a clear and organic assignment of tasks, implementing separation of functions, and inspiring and controlling the correctness of behaviour;
- formalise manual and electronic business procedures intended to regulate the performance of activities (particularly effective prevention is provided by the control tool "separation of tasks" between those who carry out the crucial phases of a risk-based process);
- assign powers of authorisation and signature in accordance with the defined organisational and management responsibilities;
- inform staff in a comprehensive, effective, clear and detailed manner of the Code of Ethics, business procedures, penalty system, powers of authorisation and signature, as well as any other appropriate means to prevent the commission of unlawful acts;
- establish a suitable penalty system;
- establish a Supervisory Body characterised by substantial autonomy and independence, whose members have the necessary professionalism to perform the required activity;
- establish a Supervisory Body that can assess the adequacy of the model, monitor its operation, ensure it is kept up to date, and act with continuity and in close connection with its business functions.

# 2. HISTORY AND PRESENTATION OF THE COMPANY

## Brief background

With over 20 years’ experience in the Industrial Ceramic and Third Firing Sector, Sicer is characterised by the high technical level of its products and its focus on innovation and aesthetic research.
Over the years, Sicer has become a world leader in the design, production and distribution of decorative materials, as well as an important point of reference for its customers, offering effective and timely assistance.
With the acquisition of the historic colour plant in Torriana (Rimini) in 2001, Sicer confirmed its desire to also become a market leader in the industrial world. Today, with numerous production sites around the world, its customers include the most prestigious international ceramic groups.

The recent recruitment of a group of industrial entrepreneurs has given Sicer additional skills to speed up its internationalisation and its plans to become a global market leader.

## Core business activities

Sicer is in the business of the production, manufacturing, packaging and trading of:

- Industrial covering and flooring products:
-
    - Frits
    - Engobes
    - Glazes
    - Printing bases
    - Grits
    - Inks
    - Digital Materials
    - Metallised laminates
    - Colouring oxides

- Products for ceramic decoration
    - Pigments for ceramic decoration
    - Printing bases and relieves
    - Precious metals and lustres
    - Metallic colours
    - Raku glazes
    - Vetrosa grits
    - Colours for decoration without firing for glass and ceramic
    - Digital decoration inks

Sicer undertakes projects in collaboration with top design firms. This gives our clients access to an internal graphic design studio, a photographic studio and a dedicated training team for external technicians.

Sicer guarantees every customer a dedicated pre-and post-sales service. We accompany our customers step-by-step in developing our products, providing specialised technical support with dedicated and loyal staff.

## Sicer case studies

*(omissis)*

# 3. PURPOSE

To ensure fairness and transparency in its business and business activities, the Company deems it necessary to adopt the model in line with the requirements of Italian Legislative Decree no. 231 of 2001.

The model is intended to describe the operating methods used and responsibilities attributed within Sicer.

The Company believes that adopting this model is more than just a legal requirement, it is a valid tool for informing and raising awareness amongst all employees and other stakeholders (consultants, partners, etc.).

The model aims to:

- prevent and reasonably limit the possible risks associated with the business, with particular regard to risks associated with illegal conduct;
- ensure that anyone operating in the name and on behalf of Sicer in the business areas at risk, is aware that committing an offence, where the provisions of the model are breached, may entail criminal and/or administrative penalties not only against them, but also against Sicer;
- reiterate that Sicer does not permit unlawful behaviour;
- make known the serious possible consequences for the company (and therefore indirectly to all stakeholders) of the application of the financial and restrictive penalties provided for in the Decree and the possibility of these being ordered as precautionary measures;
- to enable the company to constantly monitor and closely supervise the activities so that it can intervene promptly if risk situations occur and, where appropriate, apply the disciplinary measures provided for by the Model itself.

## 4. SCOPE OF APPLICATION

The rules contained in the Model apply to those who perform (even de facto) management, administration, direction or control functions in the Company, members and employees, as well as those who, while not belonging to the Company, work on its behalf or are contractually bound to it.

Consequently, the recipients of the model will include, amongst those in executive positions: 1) chairman of the BoD; 2) directors; 3) executives; 4) auditors; 5) members of the Supervisory Body; among those reporting to management: 1) employees; 2) interns.

Pursuant to specific contractual clauses and limited to the performance of sensitive activities in which they may participate, the following external parties may be given specific obligations, instrumental to the proper execution of the internal control activities provided for in this General Section:

- collaborators, agents and representatives, consultants and, in general, persons performing self-employed activities to the extent that they operate in sensitive areas of activity on behalf or in the interests of the Company;
- suppliers and trading partners (including in the form of temporary associations of companies and joint ventures) operating in a significant and/or ongoing manner within the so-called sensitive business areas on behalf or in the interests of the Company.

“External parties” must also include those who, even though they have a contractual relationship with another company in the Group, essentially operate in a significant and/or ongoing manner within the areas of sensitive activities on behalf of or in the interests of the Company.

Sicer distributes this Model using suitable means to ensure all stakeholders have a thorough knowledge of it.

The parties to which the Model is addressed are required to comply with all the provisions in a timely manner, including by fulfilling the duties of loyalty, fairness and diligence arising from the legal relationships established with the Company.

Sicer condemns any behaviour that deviates not only from the law, but also, and most importantly for our purposes, which deviates from the Model and Code of Ethics; even if the unlawful behaviour was carried out in the interest of the Company or with the intention of giving it an advantage.

# 5. RISK ASSESSMENT IN SICER

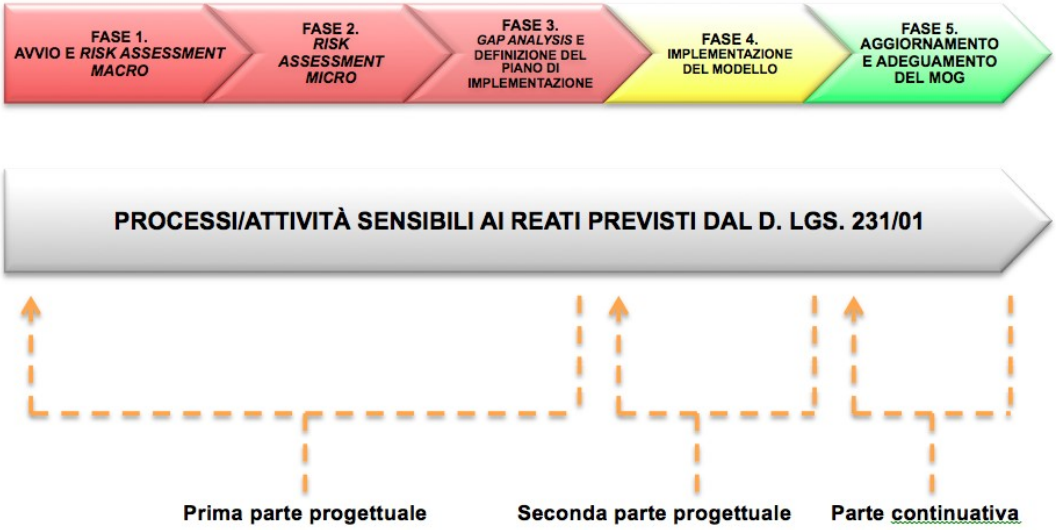
## 5.1. Summary of the project to prepare and develop the organisation, management and control model, in accordance with Italian Legislative Decree 231/2001 for the Company Sicer

In a meeting on 4 January 2017, working group 231 presented to the Company the launch of the project to develop the Company's organisation, management and control model (hereinafter the "OMCM") pursuant to art. 6, par. 2 *a)* of Italian Legislative Decree 231/01 and the Confindustria guidelines.

During the project, working group 231 significantly involved the relevant company functions – in understanding, analysing and assessing, in addition to sharing various issues – with meetings and interviews intended to collate information about the Company with a view to a detailed analysis and assessment of risk areas, and with periodic reports on the project's progress and any criticism that arose during the project.

The project to prepare and develop the OMCM was completed in 9 months (January 2017 – September 2017) in the following stages.

**Picture no. 1: Sicer organisation, management and control model**




## 5.2. Stage 1: Launch and *Macro Risk Assessment*

This stage led to the completion of the following activities:

- Organisation, planning, announcement and launch of the project to prepare and develop the OMCM;
- Collating preliminary documentation/information;

- Analysis of the company and identification of risk areas pursuant to Italian Legislative Decree 231/01 ("macro areas" of sensitive activity) and the relevant company roles/responsibilities involved;
- Analysis and assessment of Sicer's control environment to identify any gaps with regard to key components of the OMCM.

The following stage produced specific documentation for the planning, organisation, announcement and launch of the project to prepare and develop the OMCM.

## 5.3. Stage 2: *Micro Risk Assessment*

This stage led to the completion of the following activities:

- Detailed analysis of risk areas identified through interviews;
- Identification of specific risk-sensitive processes/activities pursuant to Italian Legislative Decree 231/01 arising from detailed analysis of the areas ("macro areas" of sensitive activities);
- Risk assessment by mapping sensitive processes in terms of:
    - probable and abstractly conceivable offences to which each process is exposed;
    - potential methods for carrying out the offence for each process;
    - organisational functions/company roles involved in the process;
    - level of cover – by providing preventive protocols – for processes in terms of: system of powers, information systems, documentary procedures, reporting;
    - description of the process flow.

The mapping of the processes is reported in this "General Section" and in the individual "Special Sections" of the organisation, management and control model.

## 5.4. Stage 3: *Gap Analysis* and establishing the implementation plan

This stage led to the completion of the following activities:

- Identification of the framework of preventive protocols (system-wide and specific) to be applied to each sensitive process ("macro areas" of sensitive activities) to prevent the committing of the offences provided for by Italian Legislative Decree 231/01 and subsequent integrations;
- Assessment of the mapping of sensitive processes – performed in Stage 2 – to identify the gaps in sensitive processes with respect to the framework of identified preventive protocols (*Gap Analysis*);
- Definition of the action plan to be implemented for the development of the OMCM within the Company, taking into account the gaps emerged in processes (*Micro Risk Assessment*) and the recommendations made in Stage 1 of the project in reference to the control environment and macro components of the model (*Macro Risk Assessment*).

The outcome of these activities is reported in this "General Section" and in the individual "Special Sections" of the organisation, management and control model.

## 5.5. Stage 4: implementation of the organisation, management and control model for the Company Sicer

This stage led to the completion of the following activities:

- Implementation of the action plan for improvement - defined in Stage 3 - which led to the definition, sharing and formalisation of:
    - macro components of the OMCM: code of ethics, organisational structure, system of delegation and powers, penalty system, supervisory body regulations;
    - system-wide and specific preventive protocols – and instrumental processes for each "macro area" of sensitive activity, subject to detailed analysis in the relevant "Special Sections".

- Formalisation of the organisation, management and control model pursuant to Italian Legislative Decree 231/01, reproduced in full in the appendix to this document.

The organisation, management and control model pursuant to Italian Legislative Decree 231/01 was presented to senior management and subsequently submitted to the Company's Board of Directors and approved – in its first version – by a resolution by the BoD.

# 6. STRUCTURE AND BREAKDOWN OF THE MODEL

## 6.1. Models of reference

This Model is inspired by the "Guidelines for the construction of organisation, management and control models resolved pursuant to Italian Legislative Decree 231/01" approved by Confindustria on 7 March 2002 (updated in March 2014).

The basic phases that Guidelines identify for the construction of Models can be outlined as follows:

- The first stage consists of identifying risks, i.e. analysing the company context to show where (in which areas/sectors of activity) and by what means it is possible to verify events that are harmful to the objectives set out in the Decree;
- the second stage consists of planning the control system (known as protocols scheduling training and implementing the entity's decisions) i.e. the assessment of the existing system within the entity and any adjustments in terms of the capacity to counter or reduce to an acceptable level, the risks identified.

From a conceptual point of view, reducing risk entails a duty to intervene on two determining factors: 1) the probability of the event occurring; 2) the impact of the event itself.
To operate effectively, the system outlined cannot be limited to occasional activity, but must translate into a continuous process to be repeated with particular attention to moments of change in the business.

It is, however, noted that the premise for constructing a suitable preventive control system goes through the definition of "*acceptable risk*".
While, in designing business risk control systems, a risk is considered acceptable when additional controls "cost" more than the resource being protected (e.g., common cars are equipped with an anti-theft device, not an armed guard), in the context of Italian Legislative Decree no. 231 of 2001, the economic logic of costs cannot, however, be the sole point of reference. It is therefore important, for the purposes of the application of the rules of the Decree, to allow that an effective threshold is defined that allows a limit to be placed on the quantity/quality of the preventive measures to be introduced, in order to avoid the committing of the offences under consideration. Moreover, in the absence of a predetermined acceptable risk, the quantity/quality of preventive controls that can be imposed is virtually infinite, and one can imagine the consequences in terms of business operations. Furthermore, the general principle, which can also be invoked under criminal law, of the specific enforceability of behaviour, summed up in the Latin brocard *ad impossibilia nemo tenetur*, is an indispensable reference criterion, although it often seems difficult to identify the limit in practice.

The concept of "acceptability" referred to above, regards the risks of conduct deviating from the rules of the organisational model and not the underlying work-related risks for the health and safety of workers which, according to the principles of the accident prevention legislation in force, must be entirely eliminated in relation to the knowledge acquired on the basis of technological progress and, where this is not possible, reduced to the minimum and therefore managed.

With regard to the preventive control system to be constructed with regard to the risk of committing the offences considered by Italian Legislative Decree no. 231 of 2001, the conceptual threshold of acceptability, in the cases of intentional offences, is represented by a **prevention system that cannot be circumvented unless by fraud.** This solution is in line with the logic of "fraudulent evasion" of the organisational model as an express exemption to the aforementioned legislative decree for the purposes of excluding the entity's administrative liability (art. 6, par. 1 *c*), "*persons committed the offence by **fraudulently** evading the organisation and management models*").

In contrast, in the case of the offences of involuntary manslaughter and personal injury through negligence committed in breach of the rules in force on health and safety in the workplace, the conceptual threshold of acceptability, for the purposes of exemption under Italian Legislative Decree no. 231 of 2001, is represented by conduct (not accompanied by intention to cause death/personal injury) in breach of the preventive organisational model (and the underlying mandatory requirements prescribed by accident prevention legislation), despite the prompt compliance by the relevant Supervisory Body with the supervisory obligations set out in Italian Legislative Decree no. 231 of 2001. This is because the fraudulent evasion of organisation models appears to be incompatible with the subjective element of the offences of involuntary manslaughter and personal injury by negligence, as per art. 589 and 590 of the Italian Criminal Code.

According to the Guidelines, creating a risk management system must start from the assumption the offences can still be committed once the model has been implemented. In the case of intentional offences, the model and relevant measures must be such that the offender not only has to "intend" the offence (e.g. corrupting a public official) but could only pursue their criminal intention by fraudulently (e.g. through artifice and/or deception) circumventing the entity's instructions. The measures the offender will be "forced" to take, if they wish to commit a crime, must be taken in relation to the specific activities of the entity deemed at risk and the individual offences hypothetically linked to those activities. However, in the case of negligent offences, these should be intended by the agent only as conduct and not also as an event.

The methodology for creating a risk management system that is set out below is generally applicable.
The process described above can in fact be applied to various types of risk: legal, operational, financial *reporting*, etc. This feature allows the same approach to be used where the principles of Italian Legislative Decree no. 231 of 2001 are extended to other areas. In particular, with regard to the extension of Italian Legislative Decree no. 231 of 2001 to the offences of involuntary manslaughter and personal injury through negligence committed in breach of the rules on health and safety in the workplace, it should be reiterated that the legislation in force on preventing work-related risks sets out the essential principles and criteria for managing workplace health and safety in a company and therefore, in this context, the organisation model cannot fail to include these prerequisites.

Naturally, for organisations that already have internal self-assessment procedures in place, some of which may even be certified, their application needs to be focussed, if it is not already, on all the types of risk and all the means considered by Italian Legislative Decree no. 231 of 2001. In this regard, it should be recalled that risk management is a maieutic process that companies must implement internally in what is deemed the most appropriate manner, obviously in accordance with the obligations established by law. The models prepared and

implemented at company level will therefore be the result of the methodological application, documented by each individual entity, of the instructions given here, according to its internal operational context (organisational structure, territory covered, size, etc.) and external operational context (economic sector, geographic area) as well as individual offences that are hypothetically linked to the specific activities of the entity considered at risk.

With regard to the operating methods for risk management, particularly in relation to those individuals/roles in the company that could be directly responsible for it, there are essentially two methodologies:

- assessment by a company body that performs this activity in association with line *management*;
- self-assessment by the operating *management* with support from a methodology tutor/facilitator.

According to the logical approach outlined above, below are the specific operational steps that the Company must take to activate a risk management system consistent with the requirements imposed by Italian Legislative Decree no. 231 of 2001. In describing this logical process, emphasis should be placed on the relevant outcomes of self-assessment activity carried out for the purposes of setting up the system.

***Inventory of the scope of business activities***

This stage can be carried out using different approaches, including by activity, by function or by process. It involves, in particular, the completion of a comprehensive periodic review of the company's reality, with the aim of identifying areas affected by potential offences. Regarding the offences of murder, or personal injury or serious personal injury through negligence committed in breach of the regulations on health and safety at work, it is not possible to exclude a priori any scope of activity, since this offence could, in fact, involve all members of the company.

A necessary part of this procedure for reviewing processes/functions at risk is the identification of parties subject to monitoring activity which, with regard to intentional offences, in particular exceptional circumstances, could also include those linked to the company by a merely quasi-subordinate relationship, such as agents, or other collaborative relationships such as commercial partners and their employees and collaborators.
In this regard, for the intentional offences of murder or personal injury committed in breach of the rules on health and safety at work, the parties subject to monitoring activities are all workers subject to this legislation.

In the same context, due diligence should also be performed whenever risk assessments reveal "suspect indicators" (e.g. conducting negotiations in territories with high corruption rates, particularly complex procedures, presence of new staff unknown to the entity) relating to a particular commercial operation.

Lastly, it should be highlighted that each company/sector presents its own specific areas of risk that can be identified only through timely internal analysis. However, processes in the financial area do take a particularly important position for the purposes of applying Italian Legislative Decree no. 231 of 2001.

***Analysis of potential risks***

The analysis of potential risks must concern the possible means of carrying out offences in different business areas (identified according to the process set out in the previous point). The analysis, which prepares the ground for a proper design for preventive measures, must result in a comprehensive representation of how the offences can be carried out in relation to the internal and external operating context in which the company operates.
In this regard, it is useful to take into account both the history of the entity, i.e. its past experiences, and the characteristics of the other parties operating in the same sector and, in particular, of any offences committed by them in the same branch of activity.

In particular, the analysis of the possible ways of carrying out the offences of murder and bodily injury or serious bodily injury through negligence, committed in breach of obligations regarding health and safety at work, corresponds to the assessment of work-related risks performed in accordance with the criteria set out in art. 28 Italian Legislative Decree n. 81 of 2008.

***Assessment/creation/adjustment of the preventive control system***

The activities described above are complemented by an assessment of any preventive control system already in place and its adjustment where necessary, or with the creation of such a system when the entity does not have one. The preventive control system must ensure that the risks of offences being committed, in the manner identified and documented in the previous stage, are reduced to an "acceptable level", according to the definition set out above. This means, in essence, to design what Italian Legislative Decree no. 231 of 2001 defines as *"specific protocols to plan the development and implementation of decisions by the entity in relation to offences to be prevented"*. There are many components to an internal control system (preventive), for which there are consolidated methodological references.

However, it should be reiterated that, for all entities, the preventive control system must be such that:

- in the case of intentional offences, it cannot be circumvented unless by intent;
- in the case of negligent offences, such as those incompatible with fraudulent intention, it is still breached, despite careful compliance with the supervision obligations by the relevant supervisory body.

According to the instructions provided, below is a list, with distinct references to intentional and negligent offences provided for by Italian Legislative Decree no. 231 of 2001, of what are generally held to be the **components (protocols) of a preventive control system**, that must be implemented at company level to guarantee the effectiveness of the model.

**A. Control systems to prevent intentional offences**

The most important components of the control system, according to the Guidelines proposed by Confindustria, are:

- the Code of Ethics with regard to the offences considered;
- a clear, formalised organisational system, especially with regard to the allocation of liability;
- manual and computerised (information systems) procedures to regulate the performance of activities by providing appropriate control points; of particular preventive effect in this area is the control instrument of separating tasks between those who carry out the crucial stages (activities) of a process at risk;

- powers of authorisation and signature assigned in accordance with the defined organisational and management responsibilities;
- a management control system that can provide timely signalling of the existence and the emergence of general and/or specific critical situations;
- communication to staff and their training.

**B. Control systems to prevent intentional offences of involuntary manslaughter and personal injury through negligence committed in breach of rules on health and safety at work**

Without prejudice to what has already been specified with regard to intentional offences, in this context, the most important components of the control system are:

- the Code of Ethics with regard to the offences considered;

- an organisational structure with tasks and responsibilities regarding health and safety at work formally defined in accordance with the company's organisational and functional structure, from the employer to the individual worker. Particular attention should be paid to specific individuals working in this field.
  This approach essentially involves:
  (a) the definition of the organisational and operational tasks of the company's management, executives, managers, and employees shall also set out the tasks relating to safety activities as assigned, as well as the responsibilities associated with carrying out these activities;
  b) the tasks of the health and safety officer and any health and safety operators, the workers' representative for safety, emergency management officers and the company physician are specifically documented;

- Training: the performance of tasks that may affect occupational health and safety requires adequate skill to be tested and nurtured through the provision of training to ensure that all staff, at all levels, are aware of the importance of their own conduct's compliance with the organisational model and the possible consequences of behaviour that deviates from the rules set out in the model. Specifically, each worker/ operator in the company must receive sufficient and adequate training with particular reference to his/her own job and duties. This must be done during the assumption, transfer or change of duties or the introduction of new work equipment, new technologies, and new dangerous substances and preparations. The company must organise training according to the requirements that periodically arise;

- communication and involvement: the circulation of information within the company is highly important in fostering the involvement of all stakeholders and permitting adequate awareness and engagement at all levels. Involvement should be achieved through:
  a) prior consultation on risk identification and assessment and establishing preventive measures;
  b) periodic meetings that take into account at least the requirements set out in the legislation in force, including the meetings scheduled for the company's management.

- Operational management: the control system for risks relating to health and safety at work should integrate and be consistent with the overall management of business processes. Analysis of business processes and their interrelation and risk assessment results leads to the definition of how to perform safely activities that significantly impact health and safety at work. The company, having identified the areas of intervention associated with health and safety, should ensure that their operational management is regulated.

  In this sense, particular attention should be paid to:
  a) recruitment and qualification of staff;
  b) organisation of work and positions;
  c) acquisition of goods and services used by the company and communication of necessary information to suppliers and contractors;
  d) regular and extraordinary maintenance;
  e) qualification and choice of suppliers and contractors;
  f) emergency management;
  g) procedures for addressing discrepancies between the objectives set and the rules of the control system;

- Safety monitoring system: occupational health and safety management should provide for a stage for verifying the maintenance of appropriate and effective risk prevention and protection measures. The technical, organisational and procedural prevention and protection measures taken by the company should be subject to planned monitoring.
  The preparation of a monitoring plan should be developed through:
  a) timing of checks (frequency);
  b) allocation of tasks and executive responsibilities;
  c) description of methodologies to be followed;
  d) ways to report any unusual situations.

There should therefore be provisions for systematic monitoring, the methods and responsibilities for which should be established at the same time as the methods and responsibilities for operational management are defined.

This **1st level monitoring** is generally performed by internal resources within the structure, both in self-monitoring by the operator and by the manager, but it may involve, for specialised aspects (e.g. instrumental verifications), the use of other resources inside or outside the company. It is also best if the verification of organisational and procedural measures relating to health and safety is carried out by individuals who are already defined in terms of the assignment of responsibilities (usually managers). Of particular importance is the Prevention and Protection Service, which is required to develop, within the scope of its responsibilities, systems for monitoring the measures taken.

It is also necessary for the company to conduct periodic **2nd level monitoring** of the functionality of the preventive system adopted. Functionality monitoring should allow strategic decisions to be made and should be conducted by competent staff who can ensure objectivity and impartiality as well as independence from the work sector being inspected.

According to the Confindustria Guidelines, the components described above must integrate organically into the architecture of the system that complies with a series of monitoring principles, including:

- *each operation, transaction and action must be verifiable, documented, consistent and appropriate*: for every action there must be adequate supporting documentation which can be checked at any time to verify the characteristics of the action and reasons behind it, and identify who authorised, performed, recorded, and verified the action;
- *no-one can manage an entire system independently:* the system must guarantee the application of the principle of the separation of functions, meaning that the authorisation and performance of an operation must be the responsibility of someone other than the person who performs, monitors or keeps the accounting records for the operation;
- *control documents*: the control system must document (possibly through the production of minutes) the performance of controls and supervision;

It should be highlighted that failure to comply with specific points of the Confindustria Guidelines does not in itself affect the validity of the Model. In fact, as the individual Model has to be drafted with regard to the specific reality of the company to which it refers, it may well depart from certain points in the Guidelines (which are inherently of a general nature) when further guarantees are needed with regard to the requirements protected by the Decree.

According to this observation, the exemplifying observations contained in the appendix to the Guidelines (known as the case study) as well as the summary list of the control instruments set out therein should also be evaluated.

**C. Control system to prevent environmental offences**

Without prejudice to what has already been specified with regard to intentional offences, in this context, the most important components of the control system are:

- the Code of Ethics with regard to the offences considered;

- an organisational structure with environmental tasks and responsibilities formally defined in accordance with the company's organisational and functional structure, from the legal representative to the individual worker. Particular attention should be paid to specific individuals working in this field.

  This approach essentially involves:
  a) the definition of the organisational and operational tasks of the company's management, executives, managers, and employees shall also set out the tasks relating to environmental activities as assigned, as well as the responsibilities associated with carrying out these activities;
  b) the tasks of the RSGA (Head of environmental management system) are specifically documented;

- information and training: the performance of tasks that could affect the profiles requires adequate skill to be tested and nurtured through the provision of training to ensure that all staff, at all levels, are aware of the importance of their own conduct's compliance with the organisational model and the possible consequences of behaviour that deviates from the rules set out in the model. Specifically, all the individuals involved must receive sufficient and adequate training with particular reference to his/her own job and duties. This must be done during the assumption, transfer or change of duties or the introduction of new work equipment, new technologies, and new dangerous substances and preparations. The company must organise training according to the requirements that periodically arise, and it must give notice of this training by means of documents (to be kept) which infer the content of the courses, the obligation to participate and attendance checks;

- communication and involvement: the circulation of information within the company is highly important in fostering the involvement of all stakeholders and permitting adequate awareness and engagement at all levels. Involvement should be achieved through:
  a) prior consultation on risk identification and assessment and establishing preventive measures;
  b) periodic meetings that take into account at least the requirements set out in the legislation in force, including the meetings scheduled for the company's management.

- operational management: the control system for risks relating to environment should integrate and be consistent with the overall management of business processes.

  In this sense, particular attention should be paid to:
  a) recruitment and qualification of staff;
  b) organisation of work and positions;
  c) acquisition of goods and services used by the company and communication of necessary information to suppliers and contractors;
  d) regular and extraordinary maintenance;

e) qualification and choice of suppliers and contractors;
f) procedures for addressing discrepancies between the objectives set and the rules of the control system.

- Environmental monitoring system: environmental protection management should provide for a stage for verifying the maintenance of appropriate and effective risk prevention and protection measures. The technical, organisational and procedural prevention and protection measures taken by the company should be subject to planned monitoring.

The preparation of a monitoring plan should be developed through:
a) timing of checks (frequency);
b) allocation of tasks and executive responsibilities;
c) description of methodologies to be followed;
d) ways to report any unusual situations.

There should therefore be provisions for systematic monitoring, the methods and responsibilities for which should be established at the same time as the methods and responsibilities for operational management are defined.

This **1st level monitoring** is generally performed by internal resources within the structure, both in self-monitoring by the operator and by the manager, but it may involve, for specialised aspects (e.g. instrumental verifications), the use of other resources inside or outside the company. It is also best if the verification of organisational and procedural measures relating to environmental protection is carried out by individuals who are already defined in terms of the assignment of responsibilities.

It is also necessary for the company to conduct periodic **2nd level monitoring** of the functionality of the preventive system adopted. Functionality monitoring should allow strategic decisions to be made and should be conducted by competent staff who can ensure objectivity and impartiality as well as independence from the work sector being inspected.

The components described above must integrate organically into the architecture of the system that complies with a series of monitoring principles, including:
- each operation, transaction and action must be verifiable, documented, consistent and appropriate: for every action there must be adequate supporting documentation which can be checked at any time to verify the characteristics of the action and reasons behind it, and identify who authorised, performed, recorded, and verified the action;
- no-one can manage an entire system independently: the system must guarantee the application of the principle of the separation of functions, meaning that the authorisation and performance of an operation must be the responsibility of someone other than the person who performs, monitors or keeps the accounting records for the operation;
- control documents: the control system must document (possibly through the production of minutes) the performance of controls and supervision.

## 6.2. Framework and rules for the approval of the Model and updates

The methodology used for preparing the Model was consistent with what is proposed by the Confindustria Guidelines:

- identifying so-called *sensitive* activities through the preventive examination of business documentation (articles of association, regulations, organisational charts, powers of attorney, assignments, provisions and organisational communications) and a series of interviews with individuals in charge of the different areas of business operations (i.e. those responsible for the different functions). The analysis was aimed at identifying and evaluating the specific performance of activities in which there could be illegal conduct with a risk of the alleged offences being committed. At the same time, we have evaluated the control, including preventive control, in place and any critical issues that require subsequent improvement;

- planning and implementing the necessary actions for the improvement of the control system and its adaptation to the aims pursued by the Decree, in light of and in consideration of the Confindustria Guidelines, as well as the fundamental principles of the separation of tasks and the definition of authorising powers consistent with the responsibilities assigned. At this stage, particular attention has been paid to identifying and regulating financial management and control processes in activities at risk;

- to define control protocols in cases where a potential risk has been perceived. In this sense, decision-making and implementation protocols have been defined, which express the set of rules and regulations that the individuals in charge of the operational responsibility for these activities have contributed to illustrate how best to govern the identified risk profile. The principle adopted in the creation of the control system is that for which the conceptual acceptance threshold is represented by a prevention system that cannot be circumvented unless by fraud, as indicated in the Guidelines proposed by Confindustria. The protocols are inspired by the rule of documenting and verifying the various phases of the decision-making process so that it can be traced back to the motivation that led to the decision.

The key parts of the Model are therefore:

- mapping the company's activities at risk, i.e. the activities in which it is possible for the offences provided for in the Decree to be committed;
- preparing appropriate control moments to prevent the offences provided for in the Decree being committed;
- *ex post* verification of company behaviour and the functioning of the Model with consequent periodic updates;
- the dissemination and involvement of all business levels in the implementation of behavioural rules and established procedures;
- assigning to the Supervisory Body specific supervisory tasks on the effective and correct functioning of the Model;
- the creation of a Code of Ethics.

The Model, without prejudice to the particular purposes described above and in relation to the exempting value provided for by the Decree, is part of the broader control system already in place and adopted to provide reasonable assurance with regard to achieving company targets, in accordance with laws and regulations, for the reliability of financial information and the safeguarding of assets, even against possible fraud.

In particular, with regard to the so-called *sensitive* business areas, the Company has identified the following core principles of its Model, which, by regulating these activities, are the tools for planning the preparation and implementation of Company decisions and ensuring proper control over them, even in relation to the offences to be prevented:

- separation of tasks through the proper distribution of responsibilities and appropriate levels of authorisation in order to avoid functional overlaps or operational assignments that focus critical activities on one individual;
- clear and formalised allocation of powers and responsibilities, with explicit indications of the limits of use and in accordance with the tasks assigned and the positions held within the organisational structure;
- no significant operation can be undertaken without authorisation;
- existence of appropriate behavioural rules to ensure that the company's activities are conducted in accordance with laws and regulations and the integrity of the company's assets;
- adequate procedural regulation of so-called *sensitive* business activities, so that: operational processes are defined by providing adequate documentary support to ensure that they can always be verified in terms of fairness, consistency and liability; or operational choices and decisions are always traceable in terms of characteristics and motivations, and those who have authorised, performed and verified individual activities can always be identified; or the ways financial resources are managed are guaranteed to be appropriate for preventing offences being committed; or supervision and monitoring activities on business transactions are carried out and documented; or there are security mechanisms that ensure adequate protection for physical and logical access to data and company assets; or the exchange of information between consecutive stages or processes is done in such a way as to ensure the integrity and completeness of the managed data.

The principles outlined above appear consistent with the instructions provided by the Guidelines issued by Confindustria, and are considered by the company to be reasonably suitable for preventing the crimes referred to in the Decree.

On these grounds, the Company considers it essential to guarantee the correct and specific application of the aforementioned principles of control in all the so-called *sensitive* areas of company activity identified and described in the Special Sections of this Model.

## 6.3. Basis and content of the Model

The Model prepared by Sicer is based on:

- the Code of Ethics, intended to establish general behavioural guidelines;
- the organisational structure that defines the assignment of tasks – envisaging, as far as possible, separation of functions or, as an alternative, compensatory controls - and the individuals responsible for checking the correctness of behaviour;
- the mapping of sensitive business areas, i.e. the description of the processes in which it is easiest to commit offences;
- instrumental processes in sensitive business areas, i.e. the processes used to manage financial instruments and/or substitute means that could support the committing of offences in areas at risk;
- the use of formalised business procedures aimed at regulating the correct operating procedures for assuming and implementing decisions in the various sensitive business areas;
- the details of the individuals responsible for such activities, ideally with performers and controllers in different roles, for the purpose of separating management and control tasks;
- the adoption of a system of delegation and powers consistent with the responsibilities assigned and which ensures a clear and transparent representation of the company's process for preparing and implementing decisions, according to the requirement of having one person in charge of the function;
- the identification of methodologies and tools that ensure an adequate level of monitoring and control (both direct and indirect), being the first type of control entrusted to the specific operators of a given

activity and the person in charge, as well as the second control for the company management and Supervisory body;
- the specification of information formats for the traceability of monitoring and control activities (e.g. forms, spreadsheets, reports, etc.);
- the definition of a penalty system for those who breach the rules of conduct established by the Company;
- the implementation of a plan for: 1) training executive and managerial staff working in sensitive areas, directors and the Supervisory Body; 2) informing all other stakeholders;
- the establishment of a Supervisory Body assigned the task of monitoring the effectiveness and proper functioning of the model, its consistency with objectives and its periodic updating.

The documentation relating to the model consists of the following sections:

general section: Description of the Model and the company
Special Section A – Code of ethics
Special Section B – Organisational structure
Special Section C – System of delegation and powers
Special Section D – Penalty system
Special Section E – Offences committed against the Public Administration or to the detriment of the State
Special Section F – Offences of counterfeiting money, credit cards, stamps and identity instruments or signs
Special Section G – Corporate offences
Special Section H – Crimes against the individual
Special Section I – Offences relating to safety in the workplace
Special Section J – Offences relating to receiving stolen goods, money laundering, the use of money, goods or benefits that are the proceeds of crime, and self-laundering
Special Section K – Transnational offences under law of 16 March 2006 no. 146
Special Section L – Offences relating to cybercrime and unlawful data processing
Special Section M – Breach of copyright offences
Special Section N – Crimes against industry and trade
Special Section O – Crime referred to in art. 377-bis Italian Criminal Code
Special Section P – Structure, composition, regulation and functioning of the Supervisory Body
Special Section Q – Organised crime
Special Section R – Offence of employing illegally staying third country nationals
Special Section S – Environmental offences
Special Section T – Internal regulations for the management of dependent staff and company assets
Penalties handbook

## 6.4. Code of Ethics

The Code of Ethics is the document developed and adopted autonomously by Sicer to inform all parties involved of the principles of corporate ethics, ethical commitments and responsibilities in conducting business and business activities with which the Company intends to comply. It must be respected by anyone working in Sicer or with whom the company has a contractual relationship.

The principles and rules of behaviour contained in this Model are complemented by what is set out in the Code of Ethics adopted by the Company, although the Model has a different scope to the Code given the purposes it intends to pursue by implementing the provisions of the Decree.
It should be specified that the Code of Ethics is an autonomously adopted tool which the Company can implement on a general level to express a set of principles of corporate ethics that the Company recognises as its own and which it intends to see observed by all its employees and by all those who cooperate in the pursuit of its business goals, including suppliers and customers; however, the Model meets specific requirements contained in the Decree, aimed at preventing particular types of offences being committed by acts which, apparently performed in the interest or to the advantage of the company, may entail an administrative liability under the provisions of the same Decree. However, in view of the fact that the Code of Ethics refers to principles of behaviour that are also suitable for preventing the illegal behaviour referred to in the Decree, it becomes relevant for the purposes of the Model and therefore formally constitutes an integral part of the Model itself.

The Company's Code of Ethics is given in "Special Section A: Code of Ethics".

## 6.5. Organisational structure

The organisational structure of the Company is defined by the delegation of functions and organisational arrangements (service orders, job descriptions, internal organisational directives) by the Chairman.
The Model, as well as the organisational structure of Sicer, is added to the intranet portal.
The Chief Executive Officer in charge of personnel is also required to keep the personnel structure up-to-date, and to inform the Supervisory Body of any significant changes to that organisation.
Sicer's organisational structure, which forms an integral and substantial part of the Model, is set out in "Special Section B: Organisational structure" and represents the map of the areas of the Company and the relevant functions that are assigned to each area.

## 6.6. Areas of sensitive activity, instrumental processes and decision-making process

The decision-making process regarding areas of sensitive activity must be consistent with the following criteria:

- any decision regarding operations in areas of sensitive activity, as identified below, must result from a written document;
- nevertheless, there can never be subjective identity between the person who makes a decision regarding the performance of a process in an area of sensitive activity and the person who actually brings it into being by completing it;
- there can never be subjective identity between those who decide and implement a process in an area of sensitive activity and those who have the power to allocate the economic and financial resources it requires.

Below are the main sensitive activities and the main instrumental processes, which are subject to detailed analysis in the relevant special parts.

For offences committed against the Public Administration or to the detriment of the State (Special Section E):

sensitive macro activities:
*(omissis)*

instrumental processes:
*(omissis)*

For offences of counterfeiting money, credit cards, stamps and identity instruments or signs (Special Section F):

sensitive macro activities:
*(omissis)*

For corporate offences (Special Section G):

sensitive macro activities:
*(omissis)*

instrumental processes:
*(omissis)*

For crimes against the individual (Special Section H):

sensitive macro activities:
*(omissis)*

instrumental processes:
*(omissis)*

For offences relating to safety in the workplace (Special Section I):

sensitive macro activities:
*(omissis)*

For offences relating to receiving stolen goods, money laundering, the use of money, goods or benefits that are the proceeds of crime, and self-laundering (Special Section J):

sensitive macro activities:
*(omissis)*

instrumental processes:
*(omissis)*

Transnational offences under law 16 March 2006 no. 146 (Special Section K)

sensitive macro activities:
*(omissis)*

instrumental processes:
*(omissis)*

For offences relating to cybercrime and unlawful data processing (Special Section L)

sensitive macro activities:
*(omissis)*

instrumental processes:
*(omissis)*

For Breach of copyright offences (Special Section M)
sensitive macro activities:
*(omissis)*

instrumental processes:
*(omissis)*

For crimes against industry and trade (Special Section N)

sensitive macro activities:
*(omissis)*

instrumental processes:
*(omissis)*

For the crime referred to in art. 377-*bis* Italian Criminal Code (Special Section O)

sensitive macro activities:
*(omissis)*

instrumental processes:
*(omissis)*

For organised crime (Special Section Q)

sensitive macro activities:

*(omissis)*

instrumental processes:
*(omissis)*

For the offence of employing illegally staying third-country nationals (Special Section R)

Sensitive macro activities and instrumental processes

*(omissis)*

For environmental offences (Special Section S):

sensitive macro activities:

*(omissis)*

With regard to:
- offences for the purposes of terrorism or the subversion of democratic order (art. 25-*quater* of the Decree);
- offences consisting of the practice of female genital mutilation (art. 25-*quater*. 1 of the Decree);
- offences relating to market abuse (art. 25-*sexies* of the Decree).

it is believed that the specific activity carried out by the company does not present any risk profiles that would reasonably justify the possibility of these offences being committed in the interest or benefit of the company.
In this regard, it is therefore considered proper to recall the principles contained in this General Section of the Model and in the Code of Ethics, which bind the Recipients of the Model to comply with the values of solidarity, morality, fairness and respect for the law.

### *6.6.1. Archiving documentation relating to sensitive activities and instrumental processes*

The activities carried out in the areas of sensitive activities and instrumental processes are properly formalised with particular reference to the documentation prepared during their implementation.

The documentation outlined above, produced and/or available in paper or electronic format, is filed in an orderly and systematic manner by the functions involved, or specifically identified in procedures or detailed work instructions.

In order to safeguard the company's documentary and information assets, adequate security measures are envisaged to address the risk of loss and/or alteration of documentation regarding sensitive activities and instrumental processes or unwanted access to data/documents.

### *6.6.2. Information systems and computer applications*

In order to protect the integrity of data and the effectiveness of information systems and/or computer applications used to perform operational or control activities in areas of sensitive activity or instrumental processes, or to support them, the presence and operation of the following is guaranteed:

*(omissis)*

## 6.7. Company procedures

The Company has a structure of formalised procedures to regulate the main activities.
Below, purely by way of example, is a list of some of the main procedures:
*(omissis)*

## 6.8. System of delegation and powers

The authorisation system that translates into a structured and consistent system of functions and powers within the Company must comply with the following requirements:

- delegation must combine each managerial power with the corresponding responsibility and a suitable position in the organisational chart and be updated as a result of organisational changes;
- each delegation must define and describe in a specific and unambiguous manner the managerial powers of the delegate and the individual to whom the delegate reports in the managerial hierarchy;
- the managerial powers assigned in delegation and their implementation must be in line with the business objectives;
- the delegate must have spending powers appropriate to the functions assigned to him/her;
- proxies may only be delegated to individuals with internal functional powers of attorney or a specific mandate and must include the extension of powers of representation and, where appropriate, numerical spending limits;
- only individuals with specific and formal powers can assume, in their name and on their behalf, obligations with regard to third parties;
- anyone with a relationship with the Public administration must be empowered or authorised to do so;
- the Articles of Association define the requirements and procedures for appointing the manager in charge of drawing up accounting and corporate documents.

Sicer's system of delegation and powers, which forms an integral and substantial part of the Model, is given in “Special Section C: System of delegation and powers”.

All powers conferred by delegation or execution of powers correspond exactly to duties and responsibilities as reported in the Company’s organisation chart.

## 6.9. Information and training

### *6.9.1. Information*

To guarantee the effectiveness of the Model, Sicer aims to ensure that all recipients are well informed, according to their different level of involvement in sensitive processes.

To this end, Sicer will propagate the Model using the following general means:

- creating specific, constantly updated webpages on the company's intranet site, the contents of which essentially concern:

a) general information about the Decree and the guidelines adopted for drafting the Model;
b) the structure and main operational provisions of the Model adopted by Sicer;
c) the Supervisory Body's reporting procedure and the standard form for reporting – by individuals in executive positions and by employees – any behaviour, on the part of other employees or third parties, considered to be potentially contrary to the contents of the Model.

At the time of the adoption of the Model, all employees will be sent a notice - from the bodies identified (e.g. Chairmanship, General Management, etc.) - to warn that the documents of the Organizational Model are published on the corporate website and on the corporate intranet portal. Communication will also be affixed to the corporate bulletin board.

New employees will be given the relevant information on the Model adopted including an information note, in the body of the letter of employment, regarding the Decree and the characteristics of the Model adopted.

### *6.9.2. Information to external collaborators and partners*

All individuals outside the Company (consultants, partners, etc.) will be duly informed about Sicer's adoption of a Model including a Code of Ethics. To this end, Sicer will inform all the aforementioned individuals of the internet address where the Model and the Code of Ethics can be viewed.
They will also be required to formally undertake to comply with the provisions contained in the aforementioned documents.
With regard to external consultants who work closely with Sicer, Sicer will be responsible for contacting them and ensuring, through detailed verification, that these consultants know the Company Model and are willing to respect it.

### *6.9.3. Information to Group Companies*

Group Companies must be informed of the content of the Model and of Sicer's interest so that the behaviour of all its subsidiaries complies with the provisions of the Decree. To this end, they will be informed of the adoption of this Model at the time of its adoption.

### *6.9.4. Training*

The contents of training programmes must be evaluated and endorsed by an external consultant, who is an expert in either corporate liability law (Italian Legislative Decree no. 231/2001) or, more generally, in criminal matters, who will work alongside the Supervisory Body.
Training must have a formal outline.
In general, training can also be held online, or, for employees who cannot be reached by computer, even through paper forms.

### *6.9.5. Training for so-called "executive" staff*

Training for so-called "executive" staff including members of the Supervisory Body, is based on training and refresher courses, with compulsory participation and attendance, as well as a final evaluation test - which may also be held orally – which can confirm the quality of the training received.
Training and refresher courses should be scheduled at the beginning of the year and, for newly co-opted members of the Board of Directors and new recruits in so-called "executive" positions, also based on information contained in the letter of employment.

Training of people in so-called "executive" positions should be divided into two sections: a "general" section and a "specific" one.

The "general" section must contain:

- legislative, legal and best practice references;
- the entity's administrative liability: purpose, ratio of the Decree, nature of liability, new legislation;
- recipients of the Decree;

- requirements for allocation of liability;
- description of the alleged offences;
- types of penalties applicable to the entity;
- conditions for exclusion of liability or limitation thereof.

During training, the following activities will be carried out:

- raising awareness of the importance given by Sicer to the adoption of a system of risk control and governance;
- description of the structure and contents of the Model adopted, as well as the methodological approach followed for its implementation and updating.

- The “general” section must contain:
- the precise description of the individual offences;
- the identification of offenders;
- the exemplification of the means by which offences are being committed;
- the analysis of applicable penalties;
- the combination of individual offences with the specific risk areas highlighted;
- the specific prevention protocols identified by the Company in order to avoid the occurrence of offences in identified risk areas;
- description of the behaviours to be implemented regarding communication and training of its own employees, in particular of staff working in business areas considered sensitive;
- description of the behaviours to be implemented with regard to the Supervisory Body regarding communication, reporting and collaboration in supervision and updating the Model;
- raising awareness, in those responsible for business functions potentially at risk of offence and employees reporting to them, in relation to the behaviour expected, the consequences of failure to comply and, in general, the Model adopted by Sicer.

### *6.9.6. Training other staff*

Training for other types of staff begins with an internal information note which, for new recruits, will be delivered at the time of recruitment.
Training for staff other than so-called “executive” staff is based on training and refresher courses, with compulsory participation and attendance, as well as a final evaluation test - which may also be held orally – which can confirm the quality of the training received.
Training and refresher courses should be scheduled at the beginning of the year.

Training for people other than those in so-called “executive” positions should be divided into two sections: a “general” section and a possible and/or partial “specific” section.

The “general” section must contain:

- legislative, legal and best practice references;
- the entity’s administrative liability: purpose, ratio of the Decree, nature of liability, new legislation;
- recipients of the Decree;
- requirements for allocation of liability;
- description of the alleged offences;
- types of penalties applicable to the entity;
- conditions for exclusion of liability or limitation thereof.

During training, the following activities will be carried out:

- raising awareness of the importance given by Sicer to the adoption of a system of risk control and governance;
- description of the structure and contents of the Model adopted, as well as the methodological approach followed for its implementation and updating.

The “general” section must contain:

- the precise description of the individual offences;
- the identification of offenders;
- the exemplification of the means by which offences are being committed;
- the analysis of applicable penalties;
- the combination of individual offences with the specific risk areas highlighted;
- the specific prevention protocols identified by the Company in order to avoid the occurrence of offences in identified risk areas;
- description of the behaviours to be implemented regarding communication and training of its own employees, in particular of staff working in business areas considered sensitive;
- description of the behaviours to be implemented with regard to the Supervisory Body regarding communication, reporting and collaboration in supervision and updating the Model;
- raising awareness, in those responsible for business functions potentially at risk of offence and employees reporting to them, in relation to the behaviour expected, the consequences of failure to comply and, in general, the Model adopted by Sicer.

With regard to training regarding the "specific" section, it should be said that this will only be intended for those individuals who are really at risk of carrying out activities under Italian Legislative Decree no. 231 of 2001 and limited to the areas of risk with which they may come into contact.

### *6.9.7. Training for the Supervisory Body*

Training for the Supervisory Body is arranged with an external consultant, who is an expert in either corporate liability law (Italian Legislative Decree no. 231/2001) or, more generally, in criminal matters.

This training is intended to provide the Supervisory Body with a high-level understanding - from a technical point of view - of the organisational model and the specific prevention protocols identified by the Company, as well as the necessary tools to properly perform its control duties.

This training - mandatory and controlled – can in general take the form of participating in: 1) conferences or seminars about Italian Legislative Decree no. 231 of 2001; 2) meetings with experts on corporate administrative liability (Italian Legislative Decree no. 231/2001) or criminal matters; in particular, with reference only to understanding the organisational model and the specific prevention protocols identified by the Company, by participating in training and refresher courses organised for individuals in so-called “executive” positions.
Training for the Supervisory Body must have the content of the "generalist" and "specific" training already described, as well as insights into:

- independence;
- autonomy;
- continuity of action;
- professionalism;
- relationships with company bodies;
- relationships with other bodies responsible for internal control;

- relationship between the implementation of the Model and the other control systems implemented by the company;
- anonymous reports to the Supervisory Body;
- reporting the activities of the Supervisory Body (inspection reports, meeting reports, etc.);
- examples of check lists for inspection activities;
- examples of mapping of sensitive activities and instrumental processes

## 6.10. Penalty system

The provision of an effective penalty system for breaching the requirements contained in the Model is a basic condition for ensuring the effectiveness of the model itself.

In that regard, article 6, par. 2 *e)* and art. 7 par. 4 *b)* of the Decree stipulate that the model should "introduce a suitable disciplinary system to penalise the failure to comply with the measures set out in the model".

The application of the disciplinary penalties determined under the Decree excludes the outcome of any criminal proceedings, since the rules imposed by the Model and the Code of Ethics are assumed by Sicer in full autonomy, regardless of the type of offence that breaches of the Model or of the Code itself may determine.

Specifically, Sicer's penalty system:

- is structured differently according to the recipients: individuals in so-called "executive" positions; employees; external collaborators and partners;
- identifies the exact disciplinary penalties to be adopted against those who commit violations, infringements, evasion, imperfect or partial applications of the requirements contained in the model, all in accordance with the relevant provisions of the NCBA and the applicable legislative provisions;
- provides for a specific procedure for the application of the aforementioned penalties, identifying the person in charge of their application and in general monitoring the enforcement, application and updating of the penalty system;
- introduces appropriate means of publication and dissemination.

Sicer has formulated and applied the penalty system in accordance with the principles set out above, which forms an integral and substantial part of the model as "Special Section D".

## 6.11. Offences committed against the Public Administration or to the detriment of the State

A detailed description of the analytical activities performed and the protocols adopted by Sicer in accordance with the provisions of articles 24 and 25 of the Decree is given in "Special Section E: Offences committed against the Public Administration or to the detriment of the State".

## 6.12. Offences of counterfeiting money, credit cards and stamps

A detailed description of the analytical activities performed and the protocols adopted by Sicer in accordance with the provisions of article 25-*bis* of the Decree is given in "Special Section F: Offences of counterfeiting money, credit cards, stamps and identity instruments or signs".

## 6.13. Corporate offences

A detailed description of the analytical activities performed and the protocols adopted by Sicer in accordance with the provisions of article 25-*ter* is given in "Special Section G: Corporate offences".

## 6.14. Crimes against the individual

A detailed description of the analytical activities performed and the protocols adopted by Sicer in accordance with the provisions of article 25-*quinquies* is given in “Special Section H: Crimes against the individual”.

## 6.15. Offences relating to safety in the workplace

A detailed description of the analytical activities performed and the protocols adopted by Sicer in accordance with the provisions of article 25-*septies* is given in “Special Section I: Offences relating to safety in the workplace".

## 6.16. Offences relating to receiving stolen goods, money laundering, the use of money, goods or benefits that are the proceeds of crime, and self-laundering

A detailed description of the analytical activities performed and the protocols adopted by Sicer in accordance with the provisions of article 25-*octies* is given in “Special Section J: Offences relating to receiving stolen goods, money laundering, the use of money, goods or benefits that are the proceeds of crime, and self-laundering”.

## 6.17. Transnational offences under law of 16 March 2006 no. 146

A detailed description of the analytical activities performed and the protocols adopted by Sicer in accordance with the provisions of article 10 law 16 March 2006 no. 146 is given in “Special Section K: Transnational offences under law of 16 March 2006 no. 146”.

## 6.18. Offences relating to cybercrime and unlawful data processing

A detailed description of the analytical activities performed and the protocols adopted by Sicer in accordance with the provisions of article 24-*bis* is given in “Special Section L: Offences relating to cybercrime and unlawful data processing”.

## 6.19. Breach of copyright offences

A detailed description of the analytical activities performed and the protocols adopted by Sicer in accordance with the provisions of article 25-*novies* is given in “Special Section M: Breach of copyright offences”.

## 6.20. Crimes against industry and trade

A detailed description of the analytical activities performed and the protocols adopted by Sicer in accordance with the provisions of article 25-*bis* 1 is given in “Special Section N: Crimes against industry and trade".

## 6.21. Offence set out in art. 377-*bis* Italian Criminal Code.

A detailed description of the analytical activities performed and the protocols adopted by Sicer in accordance with the provisions of article 25-*novies* is given in “Special Section O: Offence set out in art. 377-*bis* Italian Criminal Code”.

## 6.22. Organised crime

A detailed description of the analytical activities performed and the protocols adopted by Sicer in accordance with the provisions of article 24-*ter* is given in “Special Section Q: Organised crime”.

## 6.23. Offence of employing illegally staying third country nationals

A detailed description of the analytical activities performed and the protocols adopted by Sicer in accordance with the provisions of article 25-*duodecies* is given in “Special Section R: Offence of employing illegally staying third country nationals ”.

## 6.24. Environmental offences

A detailed description of the analytical activities performed and the protocols adopted by Sicer in accordance with the provisions of article 25-*undecies* is given in “Special Section S: Environmental offences”.

## 6.25. Management of financial resources

Art. 6 par. 2 c) of the Decree provides for the obligation, on the part of the Company, to draw up suitable terms for the management of financial resources to prevent offences being committed.

To this end, Sicer has adopted, within its own procedures, some key principles to be followed in the management of financial resources:

- all transactions linked to financial management must be performed using the Bank's current accounts;
- checks on balances and cash transactions must be carried out periodically;
- the department responsible for treasury management must define and keep up-to-date – in accordance with the Company's credit policy and on the basis of proper separation of tasks and accounting regularity – a specific formalised procedure for opening, using, controlling and closing current accounts;
- senior management must define the medium and long-term financial needs, the forms and sources of coverage and gives evidence of these in specific reports.
- With regard to the payment of invoices and expenditure commitments, the Company requires that:
- the invoice is checked in all its aspects (correspondence, calculations, taxation, receipt of goods or services);
- the invoice is recorded independently of the accounting records and no payment is made without the specific authorisation of the manager of the administration and finance office and of the ordering function;
- all borrowings for financing, including derivative contracts, both hedging and speculative, must be adopted by Board of Directors’ resolution.

## 6.26. Supervisory Body

In accordance with the provisions of art. 6 par. 1 b of the Decree, which stipulates that the task of supervising the functioning and observance of the Model and of making any relevant updates to the Model, shall be entrusted to a Company body with its own powers of initiative and control called the Supervisory Body. The Company has provided for the identification and appointment of that Body. For details, refer to "Special Section P: Structure, composition, regulation and functioning of the Supervisory Body".

## 6.27. Adoption of the model and Supervisory body in a Group of Companies

Companies controlled directly or indirectly by Sicer or belonging to the same group (hereinafter "the Group") must establish their own "organisation and management model", which is in line with the specifications of the Decree.

In doing so, the Group Company can take the Model adopted by Sicer as a reference, which will have to be adapted to the individual realities of each one, in particular, to the specific sensitive areas/activities identified within them.

Each Group Company must set up its own Supervisory Body.

The Supervisory Body of each Group Company:

- may, in the performance of its functions, make use of the resources allocated to Sicer's Supervisory Body, on the basis of a pre-established contractual relationship with the same and in accordance with the confidentiality obligation;
- will have to co-ordinate with Sicer's Supervisory Body to ensure the adoption and implementation of a Model that can prevent the occurrence of offences pursuant to Italian Legislative Decree no. 231 of 2001;
- must promptly notify Sicer's Supervisory Body in the event of breaches committed by Company directors;
- must communicate the Model adopted and any updates;
- must report, at least annually, to Sicer's Supervisory Body.