



**Organisation, Management and Control Model
in accordance with
Legislative Decree No. 231 of 8 June 2001
of Hitachi Vantara Italia S.r.l.**

INDEX

GENERAL PART	4
1. LEGISLATIVE DECREE NO. 231/2001 AND RELEVANT LEGISLATION	5
1.1. THE ADMINISTRATIVE LIABILITY REGIME APPLICABLE TO LEGAL PERSONS	5
1.2. SANCTIONS.....	6
1.3. ATTEMPTED CRIMES AND CRIMES COMMITTED ABROAD	7
1.4. TORT PROCEEDINGS AND REVIEW OF SUITABILITY BY THE COURT.....	8
1.5. ACTIONS EXEMPT FROM ADMINISTRATIVE LIABILITY.....	8
2. CONFINDUSTRIA GUIDELINES	9
3. ADOPTION OF THE MODEL BY HITACHI VANTARA ITALIA S.R.L.	10
3.1. CORPORATE OBJECTIVES AND MISSION	10
3.2. GOVERNANCE MODEL.....	10
3.3. ORGANISATIONAL STRUCTURE.....	10
3.4. MOTIVATIONS OF HITACHI VANTARA ITALIA IN ADOPTING THE MODEL.....	11
3.4.1. AIMS OF THE MODEL	11
3.4.2. THE PROCESS OF PREPARING AND UPDATING THE MODEL	12
3.5. DOCUMENT STRUCTURE	13
3.6. ELEMENTS OF THE MODEL	13
3.7. AMENDMENTS AND ADDITIONS TO THE MODEL.....	15
4. SUPERVISORY BODY	15
4.1. IDENTIFICATION OF THE SUPERVISORY BODY.....	15
4.2. FUNCTIONS AND POWERS OF THE SUPERVISORY BOARD.....	18
4.3. REPORTING BY THE SUPERVISORY BOARD TO THE CORPORATE BODIES	19
4.4. INFORMATION FLOWS TO THE SUPERVISORY BOARD.....	19
4.4.1. REPORTS TO THE SUPERVISORY BOARD.....	19
4.4.2. COLLECTION, STORAGE AND ACCESS TO THE SB ARCHIVE.....	21
5. STAFF TRAINING AND DISSEMINATION OF THE MODEL IN THE CORPORATE CONTEXT AND EXTERNALLY	21
5.1. STAFF TRAINING	21
5.2. INFORMATION TO STAFF.....	21
5.3. INFORMATION TO EXTERNAL COLLABORATORS AND PARTNERS	21
6. DISCIPLINARY SYSTEM AND MEASURES IN THE EVENT OF NON-COMPLIANCE WITH THE PROVISIONS OF THE MODEL	22
6.1. GENERAL PRINCIPLES	22
6.2. SANCTIONS FOR EMPLOYEES	22
6.2.1. CLERKS, WORKERS AND MIDDLE MANAGERS	22
6.2.2. MANAGERS.....	23
6.3. MEASURES AGAINST DIRECTORS AND THE SOLE AUDITOR.....	23
6.4. MEASURES AGAINST COLLABORATORS, CONSULTANTS, PARTNERS, BUSINESS PARTNERS AND OTHER EXTERNAL PARTIES.....	24

6.5.	PROCEDURE FOR THE APPLICATION OF SANCTIONS.....	24
6.5.1.	DISCIPLINARY PROCEEDINGS AGAINST NON-MANAGERIAL EMPLOYEES	24
6.5.2.	DISCIPLINARY PROCEEDINGS AGAINST MANAGERS	25
6.5.3.	DISCIPLINARY PROCEEDINGS AGAINST DIRECTORS AND THE SOLE AUDITOR.....	26
6.5.4.	PROCEEDINGS AGAINST THIRD PARTIES TO WHOM THE MODEL IS ADDRESSED.....	27
7.	GENERAL PRINCIPLES OF CONDUCT	27
	SPECIAL PART	29
1.	FUNCTION OF THE SPECIAL SECTION	30
2.	REPORTING OBLIGATIONS TO THE ODV	31
2.1.	AD HOC DISCLOSURE OBLIGATIONS	31
2.2.	REGULAR REPORTING OBLIGATIONS.....	31
3.	AREAS AT RISK OF DIRECT AND INSTRUMENTAL CRIME	33
3.1.	COMMERCIAL AND SALES ACTIVITIES.....	34
3.2.	INSTALLATION OF GOODS/SERVICES	38
3.3.	STAFF ACQUISITION, PROGRESSION AND MANAGEMENT	41
3.4.	PROCUREMENT OF GOODS AND SERVICES AND CONSULTANCY	45
3.5.	CORPORATE AFFAIRS.....	48
3.6.	ADMINISTRATION, FINANCE AND CONTROL.....	50
3.7.	FINANCIAL RESOURCES	54
3.8.	INFORMATION SYSTEMS.....	57
3.9.	HEALTH AND SAFETY AT WORK	63
3.10.	ENVIRONMENTAL ISSUES	68
3.11.	PRE-LITIGATION AND LITIGATION MANAGEMENT.....	71
3.12.	RELATIONS WITH INSTITUTIONS AND PUBLIC BODIES	73
3.13.	DONATIONS, GIFTS AND GRATUITIES.....	77

GENERAL PART

1. LEGISLATIVE DECREE NO. 231/2001 AND RELEVANT LEGISLATION

1.1. THE ADMINISTRATIVE LIABILITY REGIME FOR LEGAL PERSONS

Legislative Decree No. 231 of 8 June 2001 (hereinafter referred to as 'Decree' or 'Legislative Decree 231/01') introduced into the Italian legal system a system of administrative liability, to be borne by companies and associations with or without legal personality (hereinafter referred to as 'Entities'), for certain offences committed, in their interest or to their advantage, by

- natural persons performing functions of representation, administration or management of the Bodies themselves or of one of their organisational units with financial and functional autonomy, as well as natural persons exercising, also de facto, the management and control of the Bodies themselves;
- natural persons subject to the direction or supervision of one of the above-mentioned persons.

The administrative liability of the legal person is in addition to the (criminal) liability of the natural person who committed the offence, and both are subject to investigation in the same proceedings before the criminal court.

Prior to the entry into force of the Decree, the principle of personal criminal liability laid down in Article 27 of the Constitution precluded the possibility of judging and possibly convicting Entities in criminal proceedings in relation to offences committed in their interest, as there could only be joint and several liability in civil proceedings for any damage caused by their employees or for the civil obligation arising from the conviction of the employee's payment of a fine or fine in the event of his insolvency (Articles 196 and 197 of the Criminal Code).

The administrative liability of entities may result from the commission of the following types of offences:

- offences committed in relations with the Public Administration (Articles 24 and 25 of the Decree);
- computer crimes and unlawful processing of data (Article *24-bis* of the Decree);
- organised crime offences (Article *24-ter* of the Decree);
- offences relating to counterfeiting money, public credit cards, revenue stamps and identification instruments or signs (Article *25-bis* of the Decree);
- offences against industry and trade (Article *25-bis.1* of the Decree);
- corporate offences (Article *25-ter* of the Decree);
- offences for the purpose of terrorism or subversion of the democratic order (*25-quater* of the Decree);
- offences of female genital mutilation practices (Article *25-quater.1* of the Decree);
- offences against the individual (Article *25-quinquies* of the Decree);
- market abuse offences (Article *25-sexies* of the Decree);
- offences of culpable homicide or grievous or very grievous bodily harm committed in breach of health and safety regulations (*25-septies* of the Decree);
- offences of receiving stolen goods, money laundering and use of money, goods or benefits of unlawful origin, and selflaundering (Article *25-octies* of the Decree);
- offences relating to non-cash payment instruments (Article *25g.1* of the Decree);
- copyright infringement offences (Article *25-novies* of the Decree);
- offence of inducement not to make statements or to make false statements to the judicial authorities (Article *25-decies* of the Decree);
- environmental offences (Article *25-undecies* of the Decree);

- crime of employment of third-country nationals whose stay is irregular (Article *25-duodecies* of the Decree);
- crimes of racism and xenophobia (Article *25-terdecies* of the Decree);
- offences of fraud in sporting competitions, unlawful gaming or betting and gambling by means of prohibited devices (Article *25-quaterdecies* of the Decree);
- tax offences (Article *25-quinquiesdecies* of the Decree);
- smuggling offences (Article *25-sexiesdecies* of the Decree);
- offences against cultural heritage (Article *25-septiesdecies* of the Decree);
- laundering of cultural goods and devastation and looting of cultural and landscape assets (Article *25-duodicies* of the Decree);
- transnational offences, introduced by Law No. 146 of 16 March 2006, '*Law ratifying and executing the United Nations Convention and Protocols against Transnational Organised Crime*'¹. Other offences may in the future be included by the legislator in Legislative Decree 231/01, with the possible need to update this Model.

1.2. SANCTIONS

The sanctions provided for administrative offences are:

- financial penalties;
- disqualifying sanctions;
- confiscation;
- publication of the judgment.

In particular, the prohibitory sanctions, with a duration of no less than three months and no more than two years (without prejudice to the cases of definitive disqualification referred to in Article 16 of the Decree), are aimed at the specific activity to which the Entity's offence refers and consist of

- disqualification from exercising the activity;
- the prohibition to contract with the Public Administration, except to obtain the performance of a public service;
- suspension or revocation of authorisations, licences or concessions functional to the commission of the offence;
- exclusion from facilitations, financing, contributions and subsidies and the possible revocation of those already granted;
- the ban on advertising goods or services.

Disqualification sanctions are applied in the cases exhaustively indicated by the Decree, only if at least one of the following conditions is met:

- 1) the Entity has derived a significant profit from the offence and the offence has been committed:

¹ I reati presupposto che rilevano come reati transnazionali sono i seguenti: associazione per delinquere (articolo 416 c.p.); associazioni di tipo mafioso anche straniere (articolo 416-bis c.p.); induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (articolo 377-bis c.p.); criminal conspiracy for the purpose of smuggling foreign processed tobacco (Article 291-quater of Presidential Decree No. 43 of 23 January 1973); conspiracy for the purpose of illicit trafficking in narcotic drugs or psychotropic substances (Article 74 of Presidential Decree P.R. No 309 of 9 October 1990); smuggling of migrants (Article 12(3), (3-bis), (3-ter) and (5) of Legislative Decree No 286 of 25 July 1998); aiding and abetting (Article 378 of the Criminal Code).

- by persons in top positions; or
- by persons subject to the direction and supervision of others when the commission of the offence was determined or facilitated by serious organisational deficiencies;

2) in the event of repeated offences.

The type and duration of prohibitory sanctions are established by the judge, taking into account the seriousness of the offence, the degree of liability of the Entity and the activity carried out by the Entity to eliminate or mitigate the consequences of the offence and to prevent the commission of further offences. Instead of applying the sanction, the judge may order the continuation of the Entity's activity by a judicial commissioner.

Disqualification sanctions may be applied to the Entity as a precautionary measure, when there is serious evidence to believe that the Entity is responsible for the commission of the offence and there are well-founded and specific elements that lead to the belief that there is a concrete danger that offences of the same nature as the one for which the offence is being prosecuted may be committed (Article 45 of the Decree). Also in this case, instead of the prohibitory precautionary measure, the judge may appoint a judicial commissioner.

Failure to comply with prohibitory sanctions constitutes an autonomous offence provided for in the Decree as a source of possible administrative liability of the Entity (Article 23 of the Decree).

Monetary sanctions, applicable to all offences, are determined through a system based on "*quotas*" in a number of no less than one hundred and no more than one thousand and varying in amount between a minimum of Euro 258.23 and a maximum of Euro 1,549.37. The judge determines the number of quotas taking into account the seriousness of the offence, the degree of liability of the Entity and the activity carried out to eliminate or mitigate the consequences of the offence and to prevent the commission of further offences. The amount of the quotas is fixed on the basis of the Entity's economic and patrimonial conditions, in order to ensure the effectiveness of the sanction (Article 11 of the Decree).

In addition to the aforementioned sanctions, the Decree provides that the confiscation of the price or profit of the offence is always ordered (except for the part that can be returned to the injured party), which may also concern goods or other utilities of equivalent value, while the publication of the conviction may be ordered by the judge in the presence of a disqualification sanction.

1.3. ATTEMPTED CRIMES AND CRIMES COMMITTED ABROAD

The organisation is also liable for offences arising from attempted offences and offences committed abroad.

In the event of commission in the form of an attempt of the offences indicated in Chapter I of the Decree, the pecuniary penalties and disqualification sanctions are reduced by between one third and one half, while the imposition of sanctions is excluded in cases where the Entity voluntarily prevents the performance of the action or the realisation of the event. The exclusion of sanctions is justified, in this case, by the interruption of any relationship of identification between the Entity and the persons who assume to act in its name and on its behalf. This is a particular case of so-called 'active withdrawal', provided for in Article 56(4) of the Criminal Code.

According to the provisions of Article 4 of the Decree, an Entity based in Italy may be held liable in connection with offences - covered by the Decree itself - committed abroad, in order not to leave frequently occurring criminal conduct without a sanction, and in order to avoid easy evasion of the entire regulatory framework in question.

The prerequisites on which the Entity's liability for offences committed abroad is based are:

- a) the offence must be committed abroad by a person functionally linked to the Entity, pursuant to Article 5(1) of the Decree;
- b) the Entity must have its head office in the territory of the Italian State;

- (c) the Entity may be liable only in the cases and under the conditions provided for in Articles 7, 8, 9, 10 of the Criminal Code.

If the cases and conditions referred to in the above-mentioned articles of the criminal code exist, the Entity is liable provided that the State of the place where the act was committed does not prosecute it.

1.4. TORT PROCEEDINGS AND JUDICIAL REVIEW OF SUITABILITY

Liability for administrative offences resulting from a criminal offence is established in criminal proceedings.

Another rule laid down by the Decree, inspired by reasons of effectiveness, homogeneity and procedural economy, is that of the mandatory joinder of proceedings: the proceedings against the Entity shall remain joined, as far as possible, to the criminal proceedings instituted against the natural person who committed the offence underlying the Entity's liability.

The ascertainment of the liability of the Entity, attributed to the criminal court, takes place by means of:

- the verification of the existence of the predicate offence for the liability of the Entity;
- ascertaining the existence of an interest or advantage of the Entity in the commission of the offence by its employee or apical;
- the review of suitability of the organisational models adopted.

The judge's review of the abstract suitability of the organisational model to prevent the offences set out in the Decree is conducted according to the criterion of the so-called 'posthumous prognosis'. The judgement of suitability is, that is, formulated according to an essentially ex ante criterion, whereby the judge places himself, ideally, in the company's situation at the time when the offence occurred in order to test the suitability of the model adopted.

1.5. ACTIONS EXEMPT FROM ADMINISTRATIVE LIABILITY

However, Articles 6 and 7 of the Decree provide for specific forms of exemption from administrative liability of the Entity for offences committed in the interest or to the advantage of the Entity by both senior persons and employees.

In particular, in the case of offences committed by **persons in apical positions**, Article 6 provides for exoneration if the Entity proves that

- a) the management body has adopted and effectively implemented, prior to the commission of the offence, an organisational, management and control model capable of preventing offences of the kind committed (hereinafter the 'Model');
- b) the task of supervising the functioning of and compliance with the Model as well as proposing its updating has been entrusted to a Body of the Entity (hereinafter 'SB'), endowed with autonomous powers of initiative and control;
- c) the persons who committed the offence acted by fraudulently circumventing the aforementioned Model;
- d) there has been no omission or insufficient supervision by the Supervisory Board.

As far as non-managerial employees are concerned, Article 7 provides for exemption in the event that the Entity has adopted and effectively implemented, before the offence was committed, a Model capable of preventing offences of the kind committed.

The Decree also provides that the Model must meet the following requirements:

- identify the activities within the scope of which there is a possibility of offences being committed;
- provide for specific protocols aimed at planning the formation and implementation of the Entity's decisions in relation to the offences to be prevented;

- identify ways of managing financial resources that are suitable for preventing the commission of such offences;
- provide for information obligations vis-à-vis the Supervisory Board;
- introduce an internal disciplinary system suitable for penalising non-compliance with the measures indicated in the Model.

The same Decree provides that the Models may be adopted, guaranteeing the above requirements, on the basis of codes of conduct drawn up by representative trade associations.

2. CONFINDUSTRIA GUIDELINES

The preparation of this Model is inspired by the Guidelines issued by Confindustria for the first time on 7 March 2002 and subsequently updated over time.

The path they indicated for the elaboration of the Model can be schematised according to the following basic points:

- identification of areas at risk, aimed at verifying in which company areas/sectors offences may be committed;
- setting up a control system capable of reducing risks through the adoption of appropriate protocols. This is supported by the coordinated set of organisational structures, activities and operating rules applied by management and company personnel, aimed at providing reasonable certainty as to the achievement of the goals of a good internal control system. The most relevant components of the preventive control system proposed by Confindustria are:
 - code of ethics;
 - organisational system;
 - manual and computerised procedures;
 - powers of authorisation and signature;
 - control and management systems;
 - communications to and training of staff.

The control system must also be aligned with the following principles:

- verifiability, documentability, consistency and congruence of each operation;
- separation of functions;
- documentation of controls;
- Introduction of an adequate system of sanctions for violations of the rules and procedures laid down in the Model;
- identification of a Supervisory Board whose main requirements are:
 - autonomy and independence;
 - professionalism;
 - continuity of action.

In addition, the Guidelines provide for the obligation on the part of the corporate functions, and in particular those performing activities identified as 'at risk', to provide information to the Supervisory Board to report any anomalies or atypicalities found in the information available.

It is understood that the decision not to follow the Guidelines in certain specific points does not invalidate the validity of a Model. In fact, the latter, being drafted with reference to the peculiarities of a particular company, may deviate from the Guidelines, which by their very nature are general.

3. ADOPTION OF THE MODEL BY HITACHI VANTARA ITALIA S.R.L.

3.1. CORPORATE OBJECTIVES AND MISSION

Hitachi Vantara Italia S.r.l. a s.u. (hereinafter referred to as "Hitachi Vantara Italia" or the "Company"), is wholly owned by Hitachi Vantara Nederland B.V. (hereinafter referred to as the "Parent Company") and is part of the Hitachi Vantara Group, headquartered in Santa Clara, California, a subgroup of the Hitachi Group, with regard to the manufacture of:

- IT infrastructure solutions;
- data storage management software;
- data storage consultancy services.

The company's object, as emerges from the Chamber of Commerce certificate, is *'the purchase, sale, both wholesale and retail, marketing, in Italy and abroad, also by means of data transmission, both as licensor and/or agent and/or distributor, of computers and technology products related to computers, including software, as well as any other type of products, raw materials, plant equipment, instruments or services used in connection therewith; the supply, in any way, of services and network related to computers and technology products related to computers, including software'*.

3.2. GOVERNANCE MODEL

The Company's *corporate governance*, based on the traditional model, is structured as follows:

- Shareholders' Meeting, competent to deliberate in ordinary and extraordinary sessions on matters reserved to it by law or by the Articles of Association;
- Board of Directors, vested with the broadest powers for the administration of the Company, with the power to perform all appropriate acts for the achievement of the corporate purposes, with the exclusion of acts reserved - by law and by the Articles of Association - to the Shareholders' Meeting;
- Sole Auditor (hereinafter also referred to as the 'Controlling Body'), which is responsible for supervision:
 - compliance with the law and the articles of association as well as respect for the principles of proper administration;
 - the adequacy of the Company's organisational structure, internal control system and administrative accounting system, also with regard to the latter's reliability in correctly representing management events.
- Auditing company responsible for the statutory audit of the accounts.

3.3. ORGANISATIONAL STRUCTURE

The Company's organisational system is defined by the Country Leader, taking into account the provisions and global policies of the Parent Company, and therefore also the fact that the IT structure is common at the EMEA level and that some processes, or parts of processes, are centralised for all companies belonging to the Hitachi Vantara Group (such as those relating to the financial services centre) of reference and that, also in this logic, some resources of Hitachi Vantara Italia may be called upon to work at other companies of the Hitachi Vantara Group of reference and vice versa.

This system is inspired, in the context of the above, by the implementation of a separation of tasks, roles and responsibilities between the Functions so that none can independently follow all the stages of a process. The system is formalised and kept up-to-date in documents indicating the structure as a whole, with an indication of the Contacts for each Function, the hierarchical/functional reports and the tasks and responsibilities assigned to each Function. In this context, the Company has adopted a system of standards that complies with the principles of good management identified by ISO9001:2015 and ISO 27001:2014.

The dissemination of these documents is ensured by sending them by e-mail, as well as publishing them on the company intranet.

3.4. MOTIVATIONS OF HITACHI VANTARA ITALIA IN ADOPTING THE MODEL

The Company, in order to ensure that the conduct of those operating on its behalf or in its interest always complies with the principles of fairness and transparency in the conduct of business and corporate activities, has deemed it appropriate to proceed with the adoption of a Model, in line with the provisions of the Decree and the indications of the relevant case law, as well as on the basis of the Guidelines issued by Confindustria.

The Model has therefore been adopted in the conviction that it constitutes a valid awareness-raising tool for those who work in the interest or to the advantage of the Company.

In particular, they are considered **Addressees of** the Model and, as such and within the scope of their specific competences, are required to know and comply with it:

- the members of the Board of Directors (hereinafter referred to as 'BoD');
- the Controlling Body;
- employees and collaborators who have contractual relations with the Company, for any reason whatsoever, including occasional and/or only temporary ones.

Those who have relations of any kind with the Company (customers, suppliers, partners) are also required to comply with the principles set out in Legislative Decree 231/01 and in the Hitachi Vantara Group's 'Code of Ethics and Business Conduct'.

3.4.1. AIMS OF THE MODEL

The Model aims to

- improve the corporate governance system of the Company;
- set up a structured and organic system of prevention and control aimed at reducing the risk of commission of offences related to the company's activities, with particular regard to preventing any illegal conduct;
- determine, in those who act in the name of and on behalf of the Company, the awareness that they may incur, in the event of violation of the provisions herein, an offence liable to penal and administrative sanctions, not only against themselves but also against the Company;
- inform those who work in any capacity in the name of, on behalf of or in the interest of the Company that violation of the provisions contained in the Model will entail the application of appropriate sanctions up to and including termination of the contractual relationship;
- reiterate that the Company does not tolerate unlawful conduct, the purpose pursued or the erroneous belief of acting in its interest or to its advantage not mattering in any way, since such conduct is in any case contrary to the ethical principles to which the Company intends to adhere and therefore in conflict with its interest;
- actively censure conduct in breach of the Model through the imposition of disciplinary and/or contractual sanctions.

3.4.2. THE PROCESS OF PREPARING AND UPDATING THE MODEL

The Company, in view of the requirements of the Decree, has launched an internal project aimed at ensuring that this Model is updated.

Consequently, this update was preceded by a series of activities aimed at building a risk prevention and management system, described below:

- 1) Mapping of activities at risk. The objective of this phase was the analysis of the corporate context, in order to map the Company's areas of activity and, among these, identify the activities in which the offences provided for in the Decree may - in abstract - be committed. The identification of company activities and areas at risk was carried out through the prior examination of company documentation (organisational chart, main processes, proxies, group and company procedures, etc.) and the subsequent conduct of interviews with the main Contact Persons.
- 2) Analysis of potential risks. With reference to the mapping of activities, carried out on the basis of the specific context in which the Company operates and the relative representation of sensitive or at-risk processes/activities, the offences that could potentially be committed in the context of the Company's activities were identified. The result of this activity is summarised in the document "*Analysis of Risks 231*", in which the description of the activity and the functions involved in the management of the same, as well as the offences and risks to which the Company is exposed, are identified for each area at risk detected.
- 3) As-is analysis. Having identified the potentially applicable offences, we proceeded to analyse the existing system of preventive controls in the areas of activity at risk, in order to express the subsequent level of adequacy of the same for the prevention of the risk of offences. In this phase, therefore, a survey was carried out of the current existing internal control structures (Group policy, procedures and/or practices adopted, verifiability, documentability or 'traceability' of operations and controls, segregation of functions, etc.) through the information provided by the Company and the analysis of the documentation provided by it. The result of these activities is contained in the document "*Analysis of Risks 231*".
- 4) Identification of proposals for improving the internal control system. On the basis of the results obtained in the previous phase and the comparison with a theoretical reference model (consistent with the Decree, with the Confindustria Guidelines and with national and international best practices), the Company assessed the opportunity to carry out integration and/or improvement activities in the control system, indicating them in the document "*Analysis of Risks 231*".
- 5) Preparation of the Model. In view of the outcomes of the phases described above, the Company updated the Model.

On the basis of the Risk Assessment carried out, due to the specific operations of the Company, the activities at risk of commission of offences provided for by Legislative Decree 231/01, set out in the Special Part of this Model, were therefore identified. With reference to the areas at risk, any indirect relations, i.e. those that the Company has, or could have, through third parties, were also examined.

The following components of the preventive control system were analysed in the Risk Assessment:

- Formalised ethical principles. The Company has adopted the Code of Ethics and Compliance and the Code of Conduct of the Hitachi Vantara Group (hereinafter referred to as the 'Code of Ethics and Conduct'), which expresses its ethical values and defines, with specific reference to activities at risk of offences, general reference frameworks.
- Organisational system. The adequacy of the organisational system was assessed on the basis of the following criteria:
 - formalisation of the system;
 - clear definition of assigned responsibilities and hierarchical reporting lines;

- existence of segregation and contraposition of functions;
- correspondence between the activities actually performed and the tasks and responsibilities described in the Company's documents.
- Authorisation system. The analysis concerned the existence of authorisation and signature powers consistent with the organisational and management responsibilities assigned and/or concretely performed. The assessment was conducted on the basis of an examination of the powers of attorney issued and internal management delegations, in light of the corporate organisation chart.
- Procedures. The analysis focused on the existence of formalised procedures (also at Group level) to regulate the activities carried out by the Functions in risk areas, taking into account not only the negotiation phases, but also those of instruction and decision-making.
- Management control system. The analysis focused on the management control system in force in the Company, the subjects involved in the process and the system's ability to provide timely warning of the existence and emergence of general and/or particular critical situations.
- Monitoring and documentation management. The analysis focused on the existence of a suitable process monitoring system to verify results and any non-conformities, as well as the existence of a suitable documentation management system to allow traceability of operations.
- Disciplinary system. The analyses carried out were aimed at verifying the existence of a disciplinary system that sanctions any violation of the principles and provisions aimed at preventing the commission of offences.
- Communication/training of personnel and information to third parties. The checks were aimed at ascertaining the existence of forms of communication and training for Addressees and third parties on the subject of Legislative Decree 231/01.

3.5. DOCUMENT STRUCTURE

This Model consists of a 'General Section' and a 'Special Section'.

In the 'General Part', after a reminder of the principles of the Decree, the Confindustria Guidelines and the reasons for adopting the Model, the following are illustrated:

- the essential components of the Model, with particular reference to the Supervisory Board;
- staff training and dissemination of the Model in the corporate and non-corporate context;
- the disciplinary system and the measures to be taken in the event of non-compliance;
- the general principles of conduct .

The 'Special Section' highlights, for each identified risk area:

- a description of the potential risk profile;
- the activities at risk and the Functions involved in the areas at risk;
- specific control protocols.

In addition, the documents *Hitachi Group Code of Ethics and Compliance* and *Hitachi Group Codes of Conduct* (Appendix 1), which set out the values and behaviour to which the Recipients must adhere, form an integral part of this Model.

3.6. MODEL ELEMENTS

The elements on which the Model is based are described below.

- **Organisational system.** The company's organisational system (organisational functions/positions, missions and areas of responsibility) is defined by the Country Leader and formalised in documents drawn up and circulated to staff.
- **Authorisation system.** The Company's authorisation system is set up in accordance with the following requirements:
 - delegations and powers of attorney combine power with the relevant area of responsibility;
 - each proxy and power of attorney unambiguously defines the powers of the delegate and specifies their limits;
 - the managerial powers assigned through delegations/proxies are consistent with the company's objectives;
 - Those who act in the name and on behalf of the Company vis-à-vis third parties, and in particular the Public Administration, must be authorised to do so.

If the legal representative of the Company is investigated or charged for the commission of the predicate offence on which the entity's administrative liability depends, he/she may not proceed with the appointment of the Company's legal counsel by reason of the general and absolute prohibition on representation laid down in Article 39 of Legislative Decree 231/01². For this reason, HVI provides as a precautionary rule to prevent such a possible conflict of interest situation that - in the circumstance indicated above - it is the person *pro tempore* acting as the Company's "legal counsel" who is specifically authorised to perform any activity necessary to provide the entity with a lawyer.

- **Procedures.** Company procedures (developed where necessary for activities not delegated to other Hitachi Vantara Group companies or not regulated by Group procedures/policies), are characterised by the following elements:
 - separation, as far as possible, within each process, between the person who makes the decision, the person who authorises it, the person who executes that decision and the person who is entrusted with controlling the process;
 - written record of each relevant step in the process, including control (so-called 'traceability');
 - appropriate formalisation.
- **Management control.** The management control system is structured in accordance with the parent company's instructions and in such a way as to be able to analyse the periodic balances against the budget and then process the revisions. The system guarantees the:
 - multiple actors involved, in terms of appropriate segregation of functions for the processing and transmission of information;
 - ability to provide timely warning of the existence and emergence of critical situations through an adequate and timely system of information flows and reporting.
- **Documentation management.** Hitachi Vantara Italia's documentation is managed in a way that governs, as appropriate, the updating, distribution, recording, archiving and security management of documents and records.
- **Management of financial flows.** This management is defined on the basis of principles marked by a segregation of functions, such as to ensure that all disbursements are requested, carried out and controlled by independent functions or persons as distinct as possible, who, moreover, are not assigned other responsibilities that could lead to potential conflicts of interest. This segregation is also guaranteed with regard to incoming financial flows. Lastly, liquidity management is inspired by criteria of asset preservation, with the related prohibition of risky financial transactions.

² See Judgment of the Court of Cassation, Sec. III, 25 July 2023, No. 32110.

For the other elements on which the Model is based (Code of Ethics and Code of Conduct, Supervisory Board, disciplinary system, personnel information and training system, third party information system), see Annex 1 and the subsequent chapters of the General Section of the Model specifically dedicated thereto.

3.7. AMENDMENTS AND ADDITIONS TO THE MODEL

Since the Model is an 'act of issuance by the management body', in accordance with Article 6(1)(a) of the Decree, its adoption, as well as subsequent amendments and additions, are the responsibility of the Company's Board of Directors.

It is recognised that the Country Leader has the power to directly make changes or additions of a formal nature to the Model, by virtue of the need to ensure that it is constantly and promptly adapted to the operational and/or organisational changes that have occurred within the Company, including, for example:

- the integration of the operational macro-activities, indicated in the Special Part of the Model. In such a case, the Country Leader is required to communicate the changes to the Model to the Board of Directors at the first meeting after the changes are made;
- change of name, amalgamation or separation of certain corporate functions;
- the updating of the list of organisational headmasters.

The Supervisory Board is consulted in advance for any amendments to be made to the Model.

4. SUPERVISORY BODY

4.1. IDENTIFICATION OF THE SUPERVISORY BOARD

According to the indications of the Confindustria Guidelines, the characteristics of the Supervisory Board - in order for it to be able to perform its activities on the basis of the indications contained in Articles 6 and 7 of the Decree - must be

- a) Autonomy and independence. The requirements of autonomy and independence are fundamental so that the Supervisory Board is not directly involved in the management activities that are the subject of its control activities. These requirements can be achieved by excluding any hierarchical dependence of the SB within the Company and by providing for reporting to the Board of Directors.
- b) Professionalism. The Supervisory Board must possess technical and professional skills appropriate to the functions it is called upon to perform. These characteristics, together with independence, guarantee objectivity of judgement.
- c) Continuity of action. The Supervisory Board must:
 - monitor the Model with the necessary powers of investigation;
 - ensure that the Model is implemented and updated;
 - not to perform operational tasks that may affect the overall view of the company's activities required of them.

The Supervisory Board, established pursuant to Article 6(b) of the Decree, is a multi-subjective body, composed of three members, one of whom is the Chairman. The Board of Directors determines, upon appointment, the remuneration due to the Supervisory Board.

The assignment is communicated to all employees and collaborators of the Company.

In the performance of its tasks, this Body may avail itself of the support of the corporate Functions that, from time to time, will be deemed useful for the performance of the activities falling within its competence.

The Supervisory Board has its own Rules of Procedure aimed at regulating its functioning and the performance of its activities, with particular reference to the frequency of meetings and the manner in which they are held and recorded in minutes, the manner and timing of the scheduling of verification activities and the management of reports, as well as the collection and storage of information.

Pursuant to Article 6 of the Decree, the Supervisory Board has '*autonomous powers of initiative and control*'. In particular:

- The **autonomy and independence** that the Supervisory Board must necessarily have are ensured by the presence of two external members, one of whom acts as Chairman, who therefore have no operational duties within the Company and no interests that could conflict with the appointment, conditioning their autonomy of judgement and assessment, as well as by the fact that the Supervisory Board operates without hierarchical constraints in the context of corporate governance, reporting directly to the BoD. Furthermore, the activities carried out by the SB cannot be audited by any other corporate body or structure, without prejudice to the power-duty of the BoD to supervise the adequacy of the work carried out by the SB. To this end, the Board of Directors also grants the SB a specific annual expenditure budget, which must be used exclusively for the expenses necessary to perform its functions and of which the Body shall provide the Board of Directors with a specific report of its use;
- **professionalism** is ensured by the specific expertise on the subject of its members and by the power granted to the Body to make use, for the performance of its duties and with absolute budget autonomy, of the specific professional skills both of the various corporate Structures and of external consultants. The external members are selected from among professionals with proven expertise and experience in legal, financial and internal control matters, who have gained adequate and proven experience in the scope of application of the Decree;
- **continuity of action** is guaranteed by the fact that:
 - the Body is free to operate at the Company at the times and in the ways it deems most appropriate for the performance of the task assigned to it;
 - an internal member who does not have an operational role within the Company is part of the Supervisory Board;
 - is informed promptly and on an ongoing basis through regular and ad hoc information flows.

The Supervisory Board reports to the company's Board of Directors.

Appointment as a member of the Supervisory Board is conditional on the presence of the professional and honourability requirements, as well as the absence of causes of incompatibility with the appointment itself, such as - by way of example - kinship relations with members of the Company's bodies and top management, and potential conflicts of interest with the role and tasks that would be performed. In this context, the following constitute grounds for ineligibility of the Supervisory Board:

- have a relationship of marriage, kinship or affinity up to the fourth degree with the Company's Directors;
- entertain, directly or indirectly, economic relations and/or contractual relations, whether for a consideration or free of charge, with the Company, of such significance as to affect its autonomy of judgement;
- being the owner, directly or indirectly, of shares in the share capital of Hitachi Vantara Italia or being bound by other patrimonial relationships, such as to allow control or significant influence on the Company, or in any case to compromise its independence;
- hold proxies that could undermine their independent judgement;
- being in the legal condition of being disqualified, incapacitated, bankrupt or sentenced to a punishment entailing disqualification, even temporary, from public office or inability to exercise executive offices;

- have been subject to preventive measures ordered by the judicial authorities, without prejudice to the effects of rehabilitation;
- being subject to criminal proceedings, convicted or subject to punishment pursuant to Articles 444 et seq. of the Code of Criminal Procedure, without prejudice to the effects of rehabilitation, in relation to one of the offences set out in Legislative Decree 231/01;
- being the addressee of a penalty order for one of the offences referred to in Articles 185 and 187-bis of the Consolidated Law on Finance;
- be affected, for the Chairman, by causes of ineligibility pursuant to Articles 2399 lett. c and 2409-septiesdecies of the Italian Civil Code.

The external members of the Supervisory Board hold office for three years and remain, in any case, in office until their successors are appointed.

The termination of the office of member of the Body may also be brought about by resignation, disqualification or revocation, and in any case it will be the task of the Board of Directors to provide for replacement without delay.

The resignation of a member of the Body may be exercised at any time and must be formally notified to the Board of Directors, together with the reasons for it.

The disqualification of a member of the Body is provided for:

- if the above requirements are no longer met, i.e.
- in the event of serious infirmity rendering him unfit to perform his supervisory duties, or an infirmity which, in any event, results in his absence for a period of more than six months.

If causes of incompatibility arise, the Supervisory Board is required to formally notify the BoD; the latter, after carrying out the appropriate checks through the Legal Business Partner, establishes a term of not less than 30 days within which the situation of incompatibility must cease. Once this term has elapsed without the aforesaid situation having ceased, the BoD must declare the disqualification of the Body and adopt the appropriate resolutions.

The occurrence of causes of incompatibility may also be detected by a person other than the person concerned, who shall formally notify the Board of Directors, which shall proceed as described above.

Similarly, disqualification or incapacitation, or a serious infirmity that renders the Supervisory Board ineligible to perform its supervisory functions for a period exceeding six months, shall entail the declaration of disqualification of the Board, to be implemented in the manner defined above.

In order to guarantee the necessary stability of the SB and protect the legitimate performance of the functions and position held from unjustified removal, a member of the SB may only be removed for just cause. In this regard, 'just cause' for removal may include, by way of example:

- a serious breach of their duties as defined in the Model;
- a conviction of the Company pursuant to the Decree or a plea bargaining sentence, which has become final, where the "omitted or insufficient supervision" on the part of the Body is established, in accordance with Article 6(1)(d) of the Decree;
- a conviction or plea bargain issued against the Body for having committed one of the offences provided for in the Decree or offences of the same nature;
- the lack of one of the moral or professional requirements that constitute a *condition sine qua non* for the appointment of the Supervisory Board;
- violation of the confidentiality obligations to which the Supervisory Board is bound with regard to news and information acquired in the performance of its duties. In particular, the SB must ensure the confidentiality of the information it comes into possession of - with particular reference to the reports it receives on alleged violations of the Model - and refrain from seeking and using

confidential information, for purposes other than those indicated in Article 6 of the Decree. In any case, any information in the possession of the SB must be processed in compliance with the legislation in force on the subject and, in particular, in compliance with privacy regulations;

- the commission of conduct in violation of the Model and/or the Code of Ethics and Conduct.

Where there are serious reasons of convenience (e.g. application of precautionary measures), the Board of Directors may order - after hearing the opinion of the Single Statutory Auditor, if he is not the member of the SB concerned - the suspension from the functions of the member of the SB, promptly appointing a new member of the Body.

4.2. FUNCTIONS AND POWERS OF THE SUPERVISORY BOARD

The mission of the Company's Supervisory Board consists in supervising the effectiveness of the Model, in examining the adequacy of the Model, in analysing the maintenance over time of the Model's soundness and functioning requirements, and in taking care of the necessary updating of the Model, in the event that the analyses carried out make it necessary to make corrections and adjustments.

More specifically, it is the task of the SB:

- monitor the validity of the Model over time, promoting, also after consulting the Functions concerned, the necessary actions to ensure its effectiveness. This task includes the formulation of adaptation proposals to be forwarded to the competent Functions and the subsequent verification of the implementation and functionality of the proposed solutions;
- carrying out checks on the correct performance, at the company functions deemed to be at risk of offences, of company activities, in compliance with the adopted Model and proposing their updating and integration, if the need arises;
- carry out a review of existing authorisation and signature powers, in order to ascertain their consistency with the organisational and management responsibilities defined and to propose their update and/or amendment where necessary, as well as for the purpose of verifying that they are exercised within the scope of the assigned powers;
- propose, on the basis of the results obtained, to the competent corporate Functions/Country Leaders, the opportunity to draft, integrate and amend procedures, which adequately regulate the performance of activities, in order to implement a suitable Model;
- defining and monitoring information flows in order to be periodically updated by the persons concerned on the activities assessed to be at risk of offences;
- Ensure that the Recipients of the Model are made aware of the methods by which it is possible to send reports to the Supervisory Board concerning conduct or events that may lead to a violation of the Model or that are relevant under the regulations of Legislative Decree no. 231/01;
- implement, in accordance with the Model, an effective flow of information to the Board of Directors to enable the Body to report to it on the supervisory activity carried out;
- promote an adequate personnel training process through suitable initiatives for the dissemination of knowledge and understanding of the Model, as well as the adequate information of those who work on behalf of the Company with reference to the Code of Ethics and Conduct adopted.

In order to perform the tasks listed above, the Supervisory Board is vested with the powers listed below:

- access to any corporate document and/or information relevant to the performance of the functions assigned to it under the Decree;
- ensure that the heads of the corporate functions promptly provide the information, data and/or news requested from them;

- make use of the corporate functions that may be useful for the performance of activities within its competence;
- make use of external consultants of proven professionalism in cases where this is necessary for the performance of the activities falling within their remit, observing the provisions for the assignment of consultancy tasks;
- proceed, if necessary, to request information, as well as direct hearings of Directors, Employees, third parties.

4.3. REPORTING BY THE SUPERVISORY BOARD TO THE CORPORATE BODIES

With regard to reporting, the Company's Supervisory Board shall provide an annual written report to the Board of Directors and the Controlling Body. In particular, the reporting shall concern

- the overall activity carried out during the period, with particular reference to verification;
- the criticalities that have emerged both in terms of conduct or events within the Company and in terms of the effectiveness of the Model;
- the reports of breaches of the Model received during the period and the actions taken by the Supervisory Board itself and by the other persons concerned in response to such reports;
- activities that could not be carried out for justified reasons of time and/or resources and/or other justified impediment;
- the state of implementation of the Model with an indication of the necessary and/or appropriate corrective and improvement measures of the same and their level of implementation;
- the Activity Plan for the following period.

The Organism shall promptly report to the BoD (or to the Chairman alone if it is deemed appropriate for speedier action) on any information deemed useful for the BoD/Chairman to take urgent decisions.

4.4. INFORMATION FLOWS TO THE SUPERVISORY BOARD

Article 6(2)(d) of the Decree requires the provision in the Model of information obligations vis-à-vis the body responsible for supervising the operation of and compliance with the Model.

The obligation of a structured information flow is conceived as a tool for guaranteeing the supervisory activity on the effectiveness and efficacy of the Model and for the possible a posteriori ascertainment of the causes that made possible the occurrence of the offences provided for by the Decree, as well as for the purpose of conferring greater authority on the requests for documentation that become necessary to the Body in the course of its verifications.

It is possible to contact the Supervisory Board by addressing the communication to 'Organismo di Vigilanza di Hitachi Vantara Italia S.r.l.', at the Company's headquarters in Via del Bosco Rinnovato, 9, 20090 Assago (MI) or via the dedicated email box 'OdV.Italia@hitachivantara.com'.

For the specific information that must be mandatorily transmitted by the Functions to the Body on an ad hoc or periodic basis, please refer to Chapter 2 of the Special Section of the Model.

4.5. REPORTS TO THE SUPERVISORY BOARD (WHISTLEBLOWING)

As part of the whistleblowing system developed by the Hitachi Vantara Group, the Company provides an independent computer channel, available at <https://www.hitachivantara.com/hotline>, for anyone wishing to make a report to the Supervisory Board:

- written;

- oral via hotline (telephone).

The internal member of the Supervisory Board monitors any reports received, involving the Supervisory Board if the report relates to areas concerning the Model or relevant conduct pursuant to Legislative Decree 231/01.

If the whistleblower would like to present the report in a meeting, he/she can request this by e-mail at 'OdV.Italia@hitachivantara.com'.

These channels guarantee the confidentiality of the identity of the reporter, of the person involved, of the person in any case mentioned in the report, of the content of the report and of the relevant documentation, as well as of any other information or element of the report from which the identity of the reporter can be directly or indirectly deduced.

The Addressees of the Model are, therefore, required to report to the Supervisory Board any information, of any kind, including from third parties, of which they have become directly aware and which relates to the violation of the Model in the areas of activity at risk or to any other irregularities that are relevant under the Decree. In particular:

- the commission of offences referred to in the Decree or the performance of suitable acts aimed at their realisation;
- conduct not in line with the rules of conduct laid down in this Model;
- operations of particular importance or which present risk profiles such as to lead to the reasonable risk of offences being committed.

Reports of unlawful conduct must be circumstantiated and based on precise and concordant facts, and may be made using the appropriate channels indicated in the preceding paragraph.

The Supervisory Board shall consider all reports received, including those received anonymously, provided they are adequately substantiated; it shall assess any consequent initiatives at its reasonable discretion and responsibility, hearing, if necessary, the author of the report and/or the person responsible for the alleged violation and giving reasons in writing for any relevant decision taken.

In the event that, following the checks carried out, it is ascertained that the reported facts are grounded, the Supervisory Board communicates the results of its investigations to the company/group functions concerned, so that the most appropriate sanctioning measures can be taken, as described in the paragraph "*Disciplinary system and measures in the event of non-compliance with the provisions of the model*" of this document.

Where the criminal liability of the reporting person for the offences of defamation or slander, or his civil liability for the same, is established, even by a judgment of first instance, in cases of wilful misconduct or gross negligence, a disciplinary sanction shall be imposed on him.

The Company:

- protects those who make reports in good faith from retaliation, discrimination or penalisation, direct or indirect, for reasons related to the report;
- prohibits direct or indirect retaliatory or discriminatory acts against the whistleblower for reasons directly or indirectly linked to the report;
- guarantees the confidentiality of the identity of the whistleblower in the handling of the report, without prejudice to legal obligations and the protection of the rights of the Company or of persons wrongly accused and/or in bad faith;
- ensures that staff are aware of the reporting procedures and are able to use them, being aware of their rights and protections under the procedures adopted, through appropriate communication in the manner provided for in Chapter 5;
- shall, in the event of a proven breach of the whistleblower protection measures, as well as of unfounded reports revealed with malice or serious misconduct, identify and apply the sanction deemed most appropriate to the circumstance, in accordance with the provisions set out in Chapter 6 below.

4.6. COLLECTION, STORAGE AND ACCESS TO THE ARCHIVE OF THE VO

All the information, notifications and reports provided for in the Model are kept by the Supervisory Board in a special file, access to which is permitted under the terms set out in the Regulation of the Body.

5. STAFF TRAINING AND DISSEMINATION OF THE MODEL IN THE COMPANY CONTEXT AND EXTERNALLY

5.1. STAFF TRAINING

The Company promotes knowledge of the Model and the Code of Ethics and Conduct among employees, who are therefore required to be familiar with their contents, to observe them and to contribute to their implementation.

Human Resources, in cooperation with the Supervisory Board, manages personnel training on the contents of Legislative Decree 231/01 and the implementation of the Model.

The training course provides for training seminars in classroom / e-learning mode for management personnel and those holding powers of attorney. For the rest of the personnel, the training methods also include the possibility of using e-learning modes. Participation in the training sessions is compulsory.

The traceability of the participation in the training activity is implemented by means of the preparation of the list of participants and their signature, or by computerised means in the case of training via an e-learning platform.

Updating training sessions will be held in the event of significant changes to the Model, the Code of Ethics and Code of Conduct or relating to regulatory changes relevant to the Company's business, where the Supervisory Board does not deem it sufficient to simply disseminate the change in the manner described in paragraph 5.2 below.

5.2. INFORMATION TO STAFF

The Company, in addition to the above-mentioned training activities, provides personnel with adequate information on

- new legislation on the administrative liability of entities;
- procedural and organisational changes.

It is the responsibility of EMEA Regional Compliance, in cooperation with the Supervisory Board to take care:

- the inclusion of the Model and the Code of Ethics and Conduct on the company intranet;
- the sending of communications on amendments to the Model, the Code of Ethics and Code of Conduct, as well as on regulatory changes relevant to the Decree.

It is the responsibility of Human Resources to ensure the distribution of the Model and the Code of Ethics and Code of Conduct to new employees at the time of recruitment.

5.3. INFORMATION TO EXTERNAL COLLABORATORS AND PARTNERS

The Company also promotes knowledge of and compliance with Legislative Decree 231/01 and the Code of Ethics and Conduct among the Company's business and financial partners, consultants, agents, collaborators in various capacities and suppliers.

The information is provided, for the subjects listed above, through the communication of the existence of the Model and the Code of Ethics and Conduct and the publication on the Company's website of the General Part of the Model and the Code of Ethics and Conduct.

The Company also ensures that the contracts with the above-mentioned counterparties include appropriate contractual clauses providing for appropriate sanctions in the event of conduct not in line with Legislative Decree 231/01, up to and including the termination of the contractual obligations. Also in this case, any exceptions must be justified and brought to the attention of the Supervisory Board.

6. DISCIPLINARY SYSTEM AND MEASURES IN THE EVENT OF NON-COMPLIANCE WITH THE PROVISIONS OF THE MODEL

6.1. GENERAL PRINCIPLES

The provision of an adequate system of sanctions for the violation of the prescriptions contained in the Model is an essential condition for ensuring the effectiveness of the Model itself.

In this respect, in fact, Article 6(2)(e) of the Decree provides that the models must *'introduce a disciplinary system capable of penalising non-compliance with the measures indicated in the model'*.

For the purposes of this disciplinary system, and in compliance with the provisions of collective bargaining, where applicable, actions or conduct in breach of the Model constitute conduct subject to sanctions.

The application of disciplinary sanctions is irrespective of the commencement and/or outcome of any criminal proceedings, since the rules of conduct imposed by the Model are assumed by the Company in full autonomy and independently of the type of offence that breaches of the Model may determine.

The identification and application of sanctions must take into account the principles of proportionality and appropriateness with respect to the alleged infringement. In this respect, the following circumstances are relevant:

- type of offence alleged;
- concrete circumstances in which the offence took place;
- manner of commission of the conduct;
- gravity of the violation, also taking into account the subjective attitude of the agent;
- possible commission of several violations within the same conduct;
- possible complicity of several persons in the commission of the infringement;
- possible recidivism of the author.

It is responsibility:

- of the Supervisory Board to constantly monitor the adequacy of the disciplinary system;
- of Human Resources update the disciplinary system.

6.2. SANCTIONS FOR EMPLOYEES

6.2.1. CLERKS, WORKERS AND MANAGERS

Conduct by employees in violation of the behavioural rules of this Model, including non-compliance with company procedures, constitutes a disciplinary offence.

With reference to the sanctions that may be imposed on employees, they fall within those provided for in the applicable National Collective Agreement, in compliance with the procedures provided for in Article 7 of the Workers' Statute and any applicable special regulations.

In particular, in accordance with the current National Collective Bargaining Agreement for Metalworkers, it is provided that

- An employee who adopts a conduct that does not comply with the provisions of this Model or of the Code of Ethics and Code of Conduct shall be reprimanded verbally if such conduct is not

serious and does not produce significant effects on the functioning of the Model and is promptly detected by the employee;

- an employee who adopts a conduct that does not comply with the provisions of this Model or of the Code of Ethics and Code of Conduct shall be liable to a written reprimand if such conduct is not serious and does not produce significant effects on the functioning of the Model and is discovered as a result of controls carried out by internal subjects other than the person who committed the violation;
- An employee who engages in conduct that does not comply with the provisions of this Model or the Code of Ethics and Code of Conduct more than twice in the course of a year shall be liable to a fine not exceeding three hours' pay, where such conduct does not have a significant impact on the functioning of the Model;
- An employee who violates internal company procedures by adopting a conduct that does not comply with the provisions of this Model or of the Code of Ethics and Conduct and exposes the Company to the risk of damage or slight damage, or procures it an advantage in violation of the provisions contained in the Code of Ethics and Conduct, shall incur suspension from work and pay for up to three days;
- An employee who engages in conduct that seriously fails to comply with the provisions of this Model or the Code of Ethics and Conduct shall be liable to dismissal with notice;
- An employee shall be liable to dismissal without notice if he/she causes serious moral or material damage to the Company or carries out actions constituting an offence under the law, as a result of non-compliance with the provisions of this Model and/or the Code of Ethics and Code of Conduct, causing such a serious breach of trust that the relationship cannot be continued.

6.2.2. MANAGERS

In the event of a breach by managers of this Model or the adoption of a conduct that does not comply with its provisions, the most appropriate measures will be applied against those responsible in accordance with the provisions of the National Collective Labour Agreement in force.

In particular:

- in the event of a non-serious breach of one or more procedural or behavioural rules laid down in the Model or in the Code of Ethics and Code of Conduct, the manager is subject to a written warning to comply with them, which is a necessary condition for maintaining the fiduciary relationship with the Company;
- in the event of a serious breach of one or more provisions of the Model or of the Code of Ethics and Code of Conduct such as to constitute a material breach, the manager shall be liable to dismissal with notice;
- where the breach of one or more provisions of the Model or of the Code of Ethics and Code of Conduct is so serious as to irreparably damage the relationship of trust, not permitting the continuation, even temporary, of the employment relationship, the worker incurs the measure of dismissal without notice.

6.3. MEASURES AGAINST DIRECTORS AND THE SOLE AUDITOR

In the event of violation of the Model by the Company's Directors or Single Statutory Auditor, the Supervisory Board shall inform the Board of Directors or Single Statutory Auditor, who - depending on their respective competences - shall proceed to take the most appropriate and adequate initiatives in line with the seriousness of the violation and in accordance with the powers provided for by law and/or the Articles of Association.

6.4. MEASURES AGAINST COLLABORATORS, CONSULTANTS, PARTNERS, BUSINESS COUNTERPARTS AND OTHER EXTERNAL PARTIES

Any conduct by collaborators, consultants, partners, agents, commercial counterparties and other external parties in breach of the provisions of Legislative Decree 231/01 or of the Code of Ethics and Business Conduct within the scope of a contractual relationship may result, through the activation of appropriate clauses, in the imposition of the following sanctions: warning, application of a penalty (compensation for damages) or termination of the contractual relationship.

It is the responsibility of the company:

- see to the drafting and updating of such contractual clauses;
- ensure that such contractual clauses are included in negotiated agreements with third parties.

6.5. PROCEDURE FOR THE APPLICATION OF SANCTIONS

The procedure for the imposition of sanctions resulting from the violation of the Model and procedures differs with regard to each category of addressees as to the stage:

- of the notification of the infringement to the person concerned;
- determination and subsequent imposition of the sanction.

The procedure for the imposition of the sanction shall, in any event, commence upon receipt by the company bodies from time to time competent and indicated below, of the communication with which the Supervisory Board reports the possible relevance of the episode pursuant to Legislative Decree 231/01.

More specifically, in cases in which the Body receives a report or acquires, in the course of its supervisory activity, elements capable of configuring the danger of a breach of the Model, it is obliged to take action to carry out the assessments falling within its tasks. If such activity concerns the Single Statutory Auditor, the other members shall take care of such investigations.

Once the verification activity has been completed, the Supervisory Board assesses, on the basis of the elements in its possession, the existence of the conditions for the initiation of disciplinary proceedings, proceeding as indicated in Chapters 6.5.1 - 6.5.4 below.

6.5.1. DISCIPLINARY PROCEEDINGS AGAINST NON-MANAGEMENT EMPLOYEES

The procedure for the application of sanctions against non-managerial employees is carried out in accordance with the procedure described below as well as with the applicable regulations and the applicable collective agreement.

In particular, the Supervisory Board transmits to the Head of Human Resources a report containing:

- the particulars of the person responsible for the breach;
- the description of the conduct complained of;
- an indication of the provisions of the Model that have been violated;
- any documents and elements supporting the dispute.

The Company, through the Head of Human Resources, shall, within ten days of receiving the report, send the Employee a written dispute notice containing:

- a precise indication of the conduct found;
- the provisions of the Model that have been violated;

- notice of the employee's right to formulate any written submissions and/or justifications within five days of receipt of the notice, as well as to request the intervention of the representative of the trade union association to which the employee belongs or which he mandates.

Following any counter-arguments by the person concerned, the Head of Human Resources decides whether or not to apply a sanction, determining its extent, and gives reasons for the measure.

Sanctions may in any case not be applied before five days have elapsed from receipt of the dispute and must be imposed, by the Human Resources Manager, within ten days from the dispatch of the dispute, or in any case within such shorter period as may be envisaged by the collective agreement applicable in the specific case. If the measure is not imposed within that period, the justifications shall be deemed to have been accepted.

The relevant measure is also communicated to the Supervisory Board, which also verifies the actual application of the sanction imposed.

The Employee, without prejudice to the possibility of referring the matter to the Judicial Authority, may, within twenty days of receipt of the measure, initiate the establishment of a Conciliation and Arbitration Board, in which case the sanction shall be suspended until such time as the relevant ruling is made.

As part of the process described above, the Company's Board of Directors is to be informed of the results of internal audits and the sanction profile applied to employees.

6.5.2. DISCIPLINARY PROCEEDINGS AGAINST MANAGERS

The offence detection procedure with regard to Managers is carried out in compliance with the applicable legal provisions as well as the current National Collective Labour Agreement.

In particular, the Supervisory Board transmits a report to the Country Leader (in case the Country Leader is involved, to the Chairman of the Board of Directors) containing:

- the description of the conduct observed;
- an indication of the provisions of the Model that have been violated;
- the particulars of the person responsible for the breach;
- any documents proving the infringement and/or other evidence.

Within five days of receiving the report of the Supervisory Board, the Country Leader summons the manager concerned by means of a notice of objection containing:

- an indication of the conduct observed and the object of the violation under the Model;
- the notice of the date of the hearing and the right of the person concerned to make, also at that hearing, any written or oral comments on the facts.

Following this, the Country Leader will define the position of the person concerned, taking a reasoned decision on whether or not to apply a sanction.

If the person for whom the dispute procedure has been triggered holds an apical position with delegated powers attributed by the Board of Directors, and if the investigation activity proves his involvement in accordance with the Model, the Country Leader shall promptly inform the Board of Directors, which will decide on the revocation of the delegated powers attributed on the basis of the nature of the position and the possible sanction to be applied. The Country Leader will implement the relevant sanction procedure.

The measure imposing the sanction is communicated in writing to the person concerned, within ten days of the dispatch of the notice, or in any case within such shorter period as may be provided by the collective agreement applicable in the specific case, by the Country Leader.

As part of the process described above, the Board of Directors is to be informed in all such cases of the results of internal audits and the sanction profile applied.

The Supervisory Board, to which the measure imposing the sanction is sent for information, verifies its application.

Without prejudice to the right to appeal to the judicial authorities, those concerned in the proceedings may, within twenty days of receipt of the disciplinary measure, promote the establishment of a Conciliation and Arbitration Board, in accordance with the provisions of the collective bargaining agreement applicable to the specific case.

In the event of the appointment of such a board, the disciplinary sanction remains suspended until the ruling of that body.

6.5.3. DISCIPLINARY PROCEEDINGS AGAINST DIRECTORS AND THE SOLE AUDITOR

If the Supervisory Board finds that the Model has been violated by a person holding the office of Director, who is not linked to the Company by an employment relationship, it shall submit a report to the Board of Directors containing:

- the description of the conduct observed;
- an indication of the provisions of the Model that have been violated;
- the particulars of the person responsible for the breach;
- any documents proving the infringement and/or other evidence.

Within ten days of receiving the Supervisory Board's report, the Board of Directors convenes the member indicated by the Supervisory Board for a meeting of the Board, to be held no later than thirty days from receipt of the report.

The convocation must:

- be made in writing;
- contain an indication of the conduct complained of and the provisions of the Model that have been breached;
- notify the interested party of the date of the meeting, with a notice of the right to formulate any observations and/or deductions, both written and verbal. The convocation must be signed by the President or at least two members of the Board of Directors.

At the meeting of the Board of Directors, which the Supervisory Board is also invited to attend, the interested party shall be heard, any statements made by the latter shall be obtained and any further investigations deemed appropriate shall be carried out.

The Board of Directors, on the basis of the elements acquired, determines the penalty, if any, deemed applicable.

In the event that the entire (or more than half) Board of Directors is involved, the Supervisory Board transmits the aforementioned report to the Sole Auditor, who then convenes the Shareholders' Meeting, also inviting the members of the Board of Directors concerned to that meeting. Once the members of the BoD have been heard, the Shareholders' Meeting proceeds to impose (or not) the sanction it deems most appropriate.

The resolution of the Board of Directors and/or that of the Shareholders' Meeting, as the case may be, is communicated in writing by the Board of Directors to the person concerned as well as to the Supervisory Board

The procedure described above also applies if a breach of the Model by the Single Statutory Auditor is detected, within the limits allowed by the applicable laws. In this case, it is the Board of Directors that convenes the Shareholders' Meeting.

In cases where a violation of the Model by a Director linked to the Company by an employment relationship is discovered, the procedure provided for below shall be initiated with regard to Managers/Employees. If a sanction is imposed as a result of such proceedings, the Board of Directors shall promptly convene the Shareholders' Meeting to resolve the consequent measures.

6.5.4. PROCEEDINGS AGAINST THIRD PARTIES

In order to enable the initiatives envisaged by the contractual clauses indicated in Section 6.4 to be taken, the Supervisory Body shall send to the Head of the Department managing the contractual relationship and, for information to the Country Leader (to the Chairman of the Board of Directors if it is the Country Leader who manages the contractual relationship), a report containing

- the details of the person responsible for the violation;
- the description of the conduct complained of;
- an indication of the provisions of the Model that have been violated;
- any documents and elements supporting the dispute.

The aforementioned report, if the contract has been approved by the Board of Directors of the Company, must also be forwarded to the attention of the latter.

The Head of the Function which manages the contractual relationship, in agreement with the Legal Business Partner Function, on the basis of any determinations made in the meantime by the Country Leader/CdA, sends the person concerned a written notice containing an indication of the conduct observed as well as an indication of the contractual clause whose application is requested.

The relevant measure is communicated to the Supervisory Board, which verifies the actual application of the sanction.

7. GENERAL PRINCIPLES OF CONDUCT

This Model provides for the express prohibition for the Addressees to engage in conduct:

- such as to constitute any type of offence (even if only in the form of an attempt), including therefore also those provided for by Legislative Decree 231/01 and listed in Chapter 1.1 of this General Section;
- which, although they do not in themselves constitute offences falling within those considered above, may potentially become such;
- that do not comply with company procedures or with the principles expressed in this Model or in the Code of Ethics and Conduct.

Therefore, the Addressees of the Model are obliged to:

- behave correctly, transparently and cooperatively, in compliance with the law, the Code of Ethics and Code of Conduct, the principles contained in this Model and company procedures;
- carry out social activities in full compliance with applicable national and international laws and regulations;
- observe a conduct aimed at guaranteeing the regular operation of the Company, ensuring and facilitating all forms of management control by the Corporate Bodies, the Supervisory Board and the Control Body;
- constantly apply the rules of this Model, the Code of Ethics and Code of Conduct and the company's internal rules, keeping abreast of regulatory developments;
- ensure that no relationship is initiated with persons or entities that do not intend to conform to the Company's ethical principles;
- ensure the truthfulness, completeness and correctness of the information communicated to the Public Administration, the supervisory or control authorities in compliance with the regulations in force.

SPECIAL PART

1. FUNCTION OF THE SPECIAL PART

The Special Section of the Model aims, consistently with the principles outlined in the General Section, to define and formalise for each area of activity at risk pursuant to Legislative Decree 231/01 identified:

- the potential risk profile, i.e. the offences that may in abstract terms be committed in the area at risk and the ways in which they may be committed;
- the activities at risk and the entities involved, or the various corporate activities at risk and the corporate functions involved in their management;
- the specific control protocols that the Addressees, as identified in the General Section, are required to comply with, meaning the corporate documents that regulate the Company's operations, the specific instruments and control activities deemed relevant for the purposes of preventing the offences referred to in Legislative Decree No. 231/01, applicable to the activities and processes at risk of offence.

This Special Section applies to the Recipients of the Model as identified in the General Section thereof.

In line with what is described in Chapter 5 of the General Section, the Company shall ensure that Recipients are given adequate training on the contents of the Special Section.

As already mentioned in the General Section, in order to allow the Supervisory Board to be periodically updated by the corporate functions concerned on the activities at risk of offences, there are reporting obligations towards the Supervisory Board, summarised in Chapter 2 below.

2. DISCLOSURE OBLIGATIONS TO THE ODV

2.1. AD HOC DISCLOSURE OBLIGATIONS

Below is the information to be transmitted to the Supervisory Board when the event occurs:

- by Legal Business Partner:
 - measures taken by the judicial authorities, or by any other authority, from which it can be inferred that investigations/investigations are being carried out, even against unknown persons, for the offences or administrative offences referred to in the Decree;
 - the division of powers and the system of delegated powers adopted by the Company and any amendments affecting the same and the organisational structure of the Company;
 - writs of summons related to litigation;
 - the contractual clauses of Legislative Decree 231, following any substantial amendments;
 - the indication of third parties that have not adhered to the Code of Ethics and Business Conduct;
- by Human Resources, requests for legal assistance forwarded by managers and/or employees in the event of the initiation of legal proceedings for offences under the Decree;
- by the competent Function/Area, the form/report completed following an inspection received by representatives of the Public Administration;
- by the SPP (via the Personnel Department/Payroll Specialist), communication about any accidents/incidents at work;
- by EMEA IT Security, any information concerning IT incidents impacting the Company;
- by EMEA Regional Compliance, the reports:
 - of Internal Audit concerning audits of the Company;
 - of the auditors on the company's financial statements.

2.2. PERIODIC REPORTING OBLIGATIONS

Below is the information to be sent to the Supervisory Board on a regular basis:

- by EMEA Regional Compliance:
 - quarterly statements issued by the company contact persons identified in the MyComplianceManager tool;
 - results summarising the participation of the Company's employees in the compliance trainings conducted at the EMEA level. The submission is annual;
- by Human Resources:
 - the list of recruitments with indication of the name, job title and budget forecast and acceptance of the Code of Ethics and Conduct. It is sent every six months;
 - the list of reward measures (bonuses, awards, increases and promotions) with the name and title. Submission is semi-annual/annual;
 - evidence of disciplinary proceedings conducted and any sanctions imposed. These are sent every six months;
 - documentation of staff participation in the training carried out to implement the Model. The submission is annual;

Special Part

- by the RSPP, the minutes of the periodic meeting pursuant to Article 35 of Legislative Decree 81/08 as amended. The submission is annual;
- by Finance Manager :
 - the budget. Submission is annual;
 - budgets and forecasts. Submission is quarterly;
- by the Legal Business Partner, a quarterly report on pending litigation, with evidence of the lawyers in charge of the litigation and any settlement agreements.

3. AREAS AT RISK OF OFFENCES

In consideration of the characteristics of the Company's business activities, the operating context in which they are carried out, and the organisational and control structure adopted, the areas at risk of offences identified by the Company are as follows:

- commercial and sales activities (paragraph 3.1);
- installation of goods/services (paragraph 3.2);
- personnel acquisition, progression and management (section 3.3);
- procurement of goods, services and consultancy (section 3.4);
- corporate affairs (paragraph 3.5);
- administration, finance and control (paragraph 3.6);
- financial resources (section 3.7);
- information systems (section 3.8);
- health and safety at work (section 3.9);
- environmental issues (section 3.10);
- pre-litigation and litigation management (paragraph 3.11);
- relations with institutions and public bodies (paragraph 3.12);
- donations, gifts and gratuities (paragraph 3.13).

The identification of risk areas, or the way they are managed, may change over time, in consideration of various factors, such as:

- the extension/amendment of the offences provided for in Legislative Decree 231/01;
- a change in the organisational/corporate/business structure of the Company;
- the detection of conduct not in line with the prescriptions of the Model;
- the assessment of the inadequacy of certain provisions of the Model, which are not suitable for preventing the commission of offences in the areas at risk of offences.

Consequently, over time, as the factors highlighted above or other factors not foreseeable at the moment change, the Company will verify, also at the instigation of the Supervisory Board, the need to integrate/amend the risk areas highlighted above.

3.1. COMMERCIAL AND SALES ACTIVITIES

3.1.1 DESCRIPTION OF THE POTENTIAL RISK PROFILE

The performance of commercial and sales activities potentially exposes the Company to the direct or instrumental commission of the following offences:

- corruzione per l'esercizio della funzione (art. 318 c.p.), corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.), corruzione in atti giudiziari (art. 319-ter c.p.), corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), istigazione alla corruzione (art. 322 c.p.), embezzlement, extortion, undue inducement to give or promise benefits, bribery and incitement to bribery of members of international courts or bodies of the European Communities or international parliamentary assemblies or international organisations and officials of the European Communities and foreign states (Article 322-bis of the criminal code), bribery among private individuals (Article 2635(3) of the civil code) and incitement to bribery among private individuals (Article 2635-bis(1) of the civil code). These offences could be committed in order to obtain favours in the performance of corporate activities through the promise of money or other benefits to a public official or a person belonging to a private company, in order to acquire orders/contracts with the PA or a private individual;
- trafficking in unlawful influence (Article 346-bis of the Criminal Code). This offence could be committed if a representative of the Company or a third party, having become aware that a contract with a Public Administration is being finalised, offers to intercede with a person appointed by the Public Administration, who is an acquaintance of his, in order to allow the Company to conclude the contract on particularly advantageous terms, requesting, in return for this activity, the payment of an increased salary (in the case of an employee in the company) or other benefits (in the case of a third party);
- fraud (Article 640(2)(1) of the Criminal Code). This offence could be committed through the preparation of untrue documentation during the bidding stage, for instance by indicating untrue technical aspects or non-existing references;
- undue inducement to give or promise benefits (Article 319-quater of the Criminal Code), where a public official or a person in charge of a public service induces the Company to give or promise to give him money or other benefits, in order to obtain the award of a contract with the PA;
- money laundering (Article 648-bis of the Criminal Code), where, in the course of its sales activity, the Company sells an asset, for the production of which money, assets or other utilities deriving from a non-culpable offence were used;
- receiving stolen goods (Art. 648 of the Criminal Code), where the Company is paid by the Customer through the use of sums of illicit origin;
- criminal conspiracy and mafia-type associations, including foreign ones (Articles 416 and 416-bis of the Criminal Code), if the Company obtains the support of exponents of associations of the above types in the awarding of private and public contracts;
- sale of industrial products with false signs (Article 517 of the Criminal Code) and manufacture of and trade in goods made by usurping industrial property rights (Article 517-ter of the Criminal Code). These offences could occur if the Company, in preparing a commercial offer, used mendacious signs or usurped industrial property rights, or used designs/pieces covered by industrial property rights;
- terrorism and subversion of the democratic order (Article 25-quater of Legislative Decree 231/01), in the event that those who support the Company in its sales activities, or the beneficiaries of the goods/services provided, are directly or indirectly linked to persons intending to commit such offences;
- computer crimes and unlawful data processing, covered by Article 24-bis of Legislative Decree 231/01, including:

- offences of unauthorised access to a computer or telecommunications system (615-ter of the criminal code);
- Unauthorised possession, dissemination and installation of equipment, codes or other means of accessing computer or telecommunications systems (Article 615-quater of the criminal code).

Computer crimes could be committed through an employee's access to a competitor's servers/systems where he/she appropriates data/information useful to know the business strategies applied;

- Self-laundering (Article 648-ter.1 of the Criminal Code), in the event that the Company, following the commission or complicity in the commission of one of the aforementioned offences, as well as of other offences referred to in Legislative Decree 231/01, obtains utilities which it employs, substitutes or transfers, in such a way as to concretely hinder the identification of their criminal origin.

3.1.2 ACTIVITIES AT RISK AND ENTITIES INVOLVED

Below are the macro-activities identified by the Company as potentially at risk in its commercial and sales activities and the corporate bodies involved in their management:

- Direct Sales (Head of Sales Team activities - Functions involved Country Leader, Sales Team, Presales, Sales Operation, Global Services Operations, Professional Services, Global Delivery, Customer Support, Sales Finance, Order Management, Legal Business Partner);
- Indirect sales and management of distributors and resellers (Head of Partner&Alliance activities - Functions involved Country Leader, Sales Team, Presales, Order Management, Legal Business Partner Sales Finance);
- Management of marketing events (Head of Marketing Activities EMEA and/or Corporate - Functions involved Marketing & Communication, Country Leader, Sales Team, Presales);
- Order Management (Responsible for Order Management activities- Functions involved Country Leader, Sales Team, Presales, Sales Operation, Global Services Operations, Professional Services, Global Delivery, Customer Support, Sales Finance, Order Management, Legal Business Partner).

3.1.3 SPECIFIC CONTROL PROTOCOLS

In addition to complying with the principles expressed in the Code of Ethics and Conduct and, with reference to the management of relations with Partners, with the principles contained in the *"Hitachi Vantara Partner Code of Ethics and Business Conduct"*, the activities related to this risk area must be managed in compliance with the company/group procedures, which provide:

- identifying the Customer, the ultimate recipient of the supply, and conducting checks on its reliability (e.g. in terms of compliance with anti-money laundering regulations, international terrorism, etc.) on the basis of documents, data or information obtained from reliable and independent sources;
- the management of the development/approval phases of the offer by means of the information system that guarantees:
 - the involvement of several Functions in the preparation phase, both with regard to the definition of economic and technical aspects;
 - an adequate segregation of duties between the different Functions involved in the activities of negotiating the offer and signing the contract;
 - the determination of the sales price of goods/services and the application of any discounts:

Special Part

- based on standard price lists previously approved and configured in the system;
- requesting specific authorisation from the authorised representative in the event of prices/discounts deviating from standard price lists;
- an adequate traceability of the authorisation/approval process of tenders/contracts;
- the archiving and preservation of the documentation produced;
- the definition of general standard terms and conditions valid for all customers, and the involvement of the Legal Business Partner in case of deviations from them;
- the use of a special computer portal for the management of applications from Commercial Partners/Retailers/Distributors and for their selection;
- the selection of Business Partners/Retailers/Distributors after conducting assessments ('due diligence') based on a number of elements including:
 - the historical profile of Commercial Partners/Distributors/Retailers;
 - analysis of their structure and financial strength;
 - the concrete and real references possessed (e.g.: customers, experience in reselling activities, experience in consultancy activities, experience as systems integrator, executive capacity in the field of services, quality level of support activities);
- agreements with business partners/dealers/distributors are set out in writing, highlighting all the conditions of the agreement, and are checked and approved according to current procedures and in compliance with the powers conferred;
- defining the criteria for the recognition of rewards/incentives to Agents/Partners/Distributors/Retailers working for the company and carrying out appropriate monitoring activities on their disbursement;
- the definition of standard contractual conditions for the sale of goods/services, differentiated according to the type of product/service offered, containing in particular
 - standard general clauses used in all sales contracts;
 - software licence conditions, to protect the ownership of software and restrict its use (e.g. rules on: licensing and software; software licence for evaluation purposes; third-party software; open source software; restrictions on use; authorised copying; software assignments; termination of licences);
 - warranty, maintenance and service conditions (clauses governing, inter alia: duration and management of the warranty; management of maintenance and service plans; exclusions from warranty, maintenance and service; performance of remote monitoring services; fees and payment; limitations of liability; governing law; termination);
 - clauses for hosted services, aimed at regulating the licence rights of the software and its use by the customer in the context of hosted services;
- the provision within the scope of the various contracts of the clause of commitment to comply with Legislative Decree 231/01, with the express possibility for the Company to terminate the contract, as well as to take legal recourse, with persons who act in a manner contrary to company rules;
- acceptance by the Partner/Retailer/Distributor of the 'Hitachi Vantara Partner Code of Ethics and Business Conduct' document.

The Company also provides:

- with regard to the management of external communications and media relations:

Special Part

- that relations with the press and other media are reserved for the Country Leader and those authorised and/or delegated by him and that all information released to the media must be approved by the Parent Company and must not concern confidential information;
- adequate traceability of interviews;
- Strict controls, with regard to press releases, concerning inside information on the Company's economic and financial situation;
- with reference to the management of sponsorships, advertising activities and participation in/organisation of events:
 - a clear definition of the process followed when deciding to participate/sponsor an event, to advertise in a particular medium and how to formalise agreements with possible partners/counterparts;
 - the formalisation and approval of analyses concerning the motivations that led to the choice of a particular advertising channel or the decision to participate in a particular event;
 - the process followed when choosing and planning an event;
 - the operational methods followed in preparing, setting up and dismantling the event, identifying those involved;
 - the forms of reporting on the costs and returns resulting from the event;
 - verification, in the case of sponsorships of private entities, of the commercial and professional reliability of the partner. In any case, decisions on sponsorships must comply with budget limits and be submitted for approval to the person in charge at Parent Company level;
 - the way in which supporting documentation is stored and the control activities carried out.

3.2. INSTALLATION OF GOODS/SERVICES

3.2.1. DESCRIPTION OF THE POTENTIAL RISK PROFILE

Performing the activities of installing goods and providing services potentially exposes the Company to the commission of offences:

- corruzione per l'esercizio della funzione (art. 318 c.p.), corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.), corruzione in atti giudiziari (art. 319-ter c.p.), corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), istigazione alla corruzione (art. 322 c.p.), embezzlement, extortion, undue inducement to give or promise benefits, bribery and incitement to bribery of members of international courts or bodies of the European Communities or of international parliamentary assemblies or international organisations and of officials of the European Communities and foreign states (Article 322-bis of the Criminal Code). 322-bis of the Criminal Code), where the Company offers or promises undue benefits to a customer or other person, representative of the PA, (e.g. promise of money, incurring hospitality expenses outside the ordinary course of business, etc.) in order to obtain validation of the activity performed;
- trafficking in unlawful influence (Article 346-bis of the Criminal Code). This offence could be committed if a representative of the Company or a third party, having become aware that a contract is being performed with a Public Administration body or with a company entrusted with a public service, offers to intercede with a person in charge of such body/company, whom he knows, to allow the Company to invoice for services that have not been rendered, requesting, as consideration for this activity, the payment of an increased salary (in the case of an employee in the company) or of another benefit (in the case of a third party);
- fraud (Article 640(2)(1) of the criminal code). This offence may be committed through:
 - falsification, alteration and omission of documentary data in order to obtain the validation of activities otherwise not due;
 - falsification, alteration and omission of periodic statements to be issued to the PA in order to obtain approval for the delivery of goods/achievement of contractual objectives.
- fraud in public supply (Article 356 of the Criminal Code), where the Company delivers to a public customer a supply that is significantly different, for instance in terms of quality, from what was agreed;
- sale of industrial products with mendacious signs (Article 517 of the Criminal Code) and manufacture of and trade in goods made by usurping industrial property rights (Article 517-ter of the Criminal Code). These offences could occur if the Company, in the execution of an order, used mendacious signs or usurped industrial property rights, or used designs/pieces covered by industrial property rights;
- Undue inducement to give or promise benefits (Article 319-quater of the Criminal Code), where a public official or a person in charge of a public service of the customer for whom work is being carried out induces the Company to give or promise to give him money or other benefits, in order to obtain approval of a work progress report without the contractual objectives having been achieved or a certificate of performance without the actual delivery of material;
- bribery among private individuals (Article 2635(3) of the Civil Code) and incitement to bribery among private individuals (Article 2635-bis(1) of the Civil Code), in the event that a Company representative bribes, by offering/promising money or other benefits, the Project Manager (or other employee) of the private customer, in order to obtain, through the falsification/alteration/omission of documentary data, the validation of activities that would otherwise not be due;
- terrorism and subversion of the democratic order (Article 25-quater of Legislative Decree 231/01), in the event that those who support the Company in the provision of services, or the beneficiaries

of the services provided by the Company, are directly or indirectly linked to persons intending to commit such offences;

- computer crimes and unlawful data processing, covered by Article 24-bis of Legislative Decree 231/01, including:
 - offences of unauthorised access to a computer or telecommunications system (615-ter of the criminal code);
 - Unauthorised possession, dissemination and installation of equipment, codes or other means of accessing computer or telecommunications systems (Article 615-quater of the criminal code);

and certain offences relating to copyright infringement covered by Article 25-novies of Legislative Decree 231/01, including:

- Unauthorised duplication, for profit, of computer programmes;
- import, distribution, sale or possession for commercial or business purposes or rental of programmes contained in media not marked by the SIAE.

Computer offences could be committed through an employee's access to the customer's servers/systems in which he/she appropriates data/information for use to the Company's advantage, or in the introduction of malware into the customer's systems that require maintenance by the Company that would not otherwise be necessary. The unauthorised duplication of a computer programme could be committed by an employee in order to be able to review the programme abusively, thereby procuring an advantage for the Company;

- issuing invoices or other documents for non-existent transactions (Article 25-quinquiesdecies of Legislative Decree 231/01 - Article 8, paragraphs 1 and 2-bis of Legislative Decree 74/00). This offence could be committed if, in order to allow a third party to evade income tax or value added tax, it issues invoices or other documents for operations never performed, in exchange for the recognition by the third party of an economic advantage for the Company such as, for example, the approval of an order variant by the Customer;
- Self-laundering (Article 648-ter.1 of the Criminal Code), in the event that the Company, following the commission or complicity in the commission of one of the aforementioned offences, as well as of other offences referred to in Legislative Decree 231/01, obtains utilities which it employs, substitutes or transfers, in such a way as to concretely hinder the identification of their criminal origin.

3.2.2. ACTIVITIES AT RISK AND ENTITIES INVOLVED

Below are the macro-activities identified by the Company as potentially at risk in the installation of goods/services and the corporate bodies involved in their management:

- Installation and configuration of machinery and customer management (work progress, maintenance, etc.) (Responsible for Customer Support activities - function involved Global Delivery);
- Professional services delivery and customer management (work progress, maintenance, etc.) (Head of Global Delivery activities - Functions involved Global Services Operations, Professional Services).

3.2.3. SPECIFIC CONTROL PROTOCOLS

In addition to complying with the principles set out in the Code of Ethics and Code of Conduct, the activities connected with this risk area must be managed in compliance with the company/group procedures, which provide:

Special Part

- the management of orders through the support of the information system ('Sales Force'), which guarantees the traceability of all operations;
- checking the availability of the products ordered, scheduling delivery to the customer's premises and dealing with related issues;
- the involvement, where necessary, of different corporate functions to plan the activities to be carried out and of the client to analyse and prepare all the technical details related to the activities to be performed;
- carrying out maintenance activities on the equipment installed at customers' premises after checking the condition of the equipment;
- during the delivery of the equipment to the customer and before its installation, carrying out checks on the conformity of the material delivered with respect to the order received and its status;
- the periodic verification of the progress of the work, duly minuted, and the monitoring of the correct execution (testing/validation) of product installation/service provision activities;
- formalisation of the activities carried out by completing the 'Installation Report' and 'Uninstallation Report';
- Centralisation and rationalisation of the acceptance and handling of all types of calls to Hitachi Vantara technical support;
- Automatic verification of the contractual status in the take-over and opening phase of the customer call (via Hi-track and direct), which allows Salesforce to assess and decide whether or not to accept the call in the absence of an active maintenance contract.

3.3. STAFF ACQUISITION, PROGRESSION AND MANAGEMENT

3.3.1. DESCRIPTION OF THE POTENTIAL RISK PROFILE

The process of personnel acquisition, career progression and management may theoretically entail the risk of commission of offences:

- of terrorism and subversion of the democratic order (Article 25-quater of Legislative Decree 231/01), in the event that funds are directly or indirectly, but nevertheless voluntarily, provided in favour of persons intending to commit terrorist offences, through, for example, the hiring of persons belonging to/approached by associations with such aims or the allocation of bonuses/other incentives not due to such persons;
- employment of third-country nationals whose stay is irregular (Article 25-duodecies of Legislative Decree 231/01), in the event that the Company hires and employs foreign staff who do not have a residence permit. This offence may also be committed during the course of the employment relationship, if the worker's residence permit expires during that period;
- criminal association (Article 416 of the Criminal Code) of a mafia type, including a foreign one (Article 416 bis of the Criminal Code), in the event that people traceable to it are hired or career advancements are granted or bonuses/other incentives not due are attributed to personnel traceable to it.

The process of selection, career progression and personnel management also constitutes one of the instrumental ways through which, in principle, offences could be committed:

- corruzione per l'esercizio della funzione (art. 318 c.p.), corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.), corruzione in atti giudiziari (art. 319-ter c.p.), corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), istigazione alla corruzione (art. 322 c.p.), embezzlement, extortion, undue induction to give or promise benefits, bribery and incitement to bribery of members of European Community bodies and officials of the European Community and foreign states (Article 322-bis of the Criminal Code), extortion (Article 317 of the Criminal Code) and undue induction to give or promise benefits (Article 319-quater of the Criminal Code);
- trafficking in unlawful influence (Article 25 of Legislative Decree 231/01 - Article 346-bis of the criminal code);
- inducement not to make statements or to make false statements to the judicial authorities (Article 377-bis of the criminal code);
- bribery among private individuals (Article 2635(3) of the Civil Code) and incitement to bribery among private individuals (Article 2635-bis(1) of the Civil Code).

With regard to the possible ways in which such offences may be committed, the following is given as an example:

- in the selection phase, the recruitment or promise of recruitment, even through an intermediary, of a person who is 'close' or 'liked' to public/private persons to be bribed in order to obtain favours in the performance of activities (e.g.: obtaining authorisations from public persons, even through someone exercising unlawful influence, awarding orders, obtaining better conditions for a supply, etc.), not based on strictly meritocratic criteria;
- at the stage of career progression and personnel management, the acknowledgement or promise, even through an intermediary, of
 - promotions/career advancements/increases in salary/other benefits to personnel 'close to' or 'liked' by public or similar persons or private persons for corrupt purposes, not informed by strictly meritocratic criteria;
 - bonuses/incentives 'falsified/inflated' in order to make available sums of money that could be used for corrupt purposes, either directly through the crediting by the employee of the sum, or part of it, to an account in the name of a foreign company belonging to the public

official/private individual to be bribed, or indirectly through the creation of hidden funds available to the Company;

- as regards the offence of inducement not to make statements or to make false statements to the judicial authority, it could, for instance, be committed through the hiring of a person 'close' to the person who is required to make statements to the judicial authority or through the awarding of an 'inflated' bonus or the promotion of a person 'liked' by the person who is required to make statements to the judicial authority.

3.3.2. ACTIVITIES AT RISK AND ENTITIES INVOLVED

Below are the main activities identified by the Company as potentially at risk in the acquisition, progression and management of personnel and the corporate bodies involved in their management:

- Personnel selection, management and training (Head of Human Resources activities);
- Management of payroll, holidays and leave, expense reimbursements, disbursement of bonuses and commissions, and the related relations with the external consultant (Human Resources Manager, Payroll Specialist and Country Leader - Functions involved Sales Finance);
- Management of company cars and fuel cards (Payroll Specialist - Functions involved Country Leader, Sales Finance).

3.3.3. SPECIFIC CONTROL PROTOCOLS

Activities related to this risk area must be managed in compliance with the Code of Ethics and Code of Conduct, as well as with company/group procedures, which provide:

- with regard to the selection and recruitment process:
 - the management of requests for new personnel and of the selection process by means of appropriate information systems that ensure proper authorisation procedures and traceability of operations;
 - requests for new personnel must find adequate provision and coverage in the staffing requirement budget approved by the Board of Directors; otherwise, a revision of the budget, to be approved by the Top Management, must be carried out before starting the selection and recruitment process;
 - In the phase of identifying the candidate to be recruited, the involvement of a variety of actors must be envisaged. In addition, this phase must be guaranteed:
 - the traceability of the sources of curricula when acquiring and managing them (e-recruitment, advertisements, spontaneous applications, internal presentations, etc.);
 - monitoring, in the event of the use of a temporary agency for the recruitment of candidates, the way in which the agency is activated on its work;
 - the identification of a shortlist of candidates, as far as possible in view of the type of professionalism to be recruited;
 - both the technical and psycho-aptitude assessment of the candidate;
 - the assignment of responsibility for the various types of evaluation to separate individuals;
 - carrying out background checks on the selected candidate with regard to studies conducted and previous work experience, as well as a 'global sanction check';
 - the signing by the selected candidate of a declaration of absence of conflicts of interest, in particular in cases of ongoing (or previous three years') relations with the

Company (directly or by relatives within the second degree), as: representative of the PA with decision-making power; client/supplier/partner;

- The following activities must be foreseen at the offer formulation and recruitment stage:
 - o verify the existence of documentation proving that the previous steps were carried out correctly, by a person other than the applicant or the person who actively participated in the selection;
 - o ensure that the definition of economic conditions is consistent with the position held by the candidate and the responsibilities/tasks assigned to him/her;
 - o provide that the contract of employment be signed by a person with an appropriate power of attorney;
 - o verify, in case of employment of non-EU staff, the regularity of the residence permit;
 - o define a set of documents to be requested from the candidate prior to employment to verify the existence of appropriate ethical and moral requirements;
- at the time of recruitment, the following activities must be envisaged:
 - o providing the newly recruited with training on the contents of the Model and the Code of Ethics and Conduct;
 - o obtaining the declaration of receipt and undertaking to comply with the contents of the documents referred to in the previous point;
 - o information to the newly recruited in relation to:
 - characteristics of the function and tasks to be performed;
 - regulatory and salary elements, as regulated by the National Collective Labour Agreement and any company regulations;
 - rules and procedures to be adopted to avoid possible health risks associated with the work activity;
 - o communication of employment to the outsourcer in order to fulfil obligations to the relevant public bodies;
- the filing in paper/informatic format of the data/documents/acts, through the creation of a special file for each employee, prepared during selection activities, to ensure the traceability of the selection and recruitment process;
- with regard to the personnel management process:
 - the definition of the main activities as well as roles and responsibilities in the personnel management process;
 - adequate attendance recording and verification systems ;
 - the definition of rules for the management of requests and the granting of authorisations for holidays and leave, for sickness notifications and for everything concerning the determination of personnel costs;
 - the authorisation of travel and the reimbursement of related expenses, providing in particular for
 - o the modalities for authorising travel by means of a special application system;
 - o the submission by employees to their supervisor of an 'expense report' summarising the expenses incurred during the travel with the relevant receipts attached;

Special Part

- the types and limits of reimbursable expenses and the procedures for their implementation, reporting, verification, authorisation, registration and reimbursement;
- the incurring of travel expenses through the use of any company credit cards/fuel cards and the reporting thereof;
- the definition, formalisation and implementation of a staff performance appraisal system, with the support of appropriate IT tools;
- the definition, approval and disbursement of any remuneration policy measures (e.g. *"ad personam bonuses"*, salary increases), on the basis of the employee performance appraisal process referred to in the previous point and in accordance with the pre-established budget limits, with the involvement of the competent Group functions;
- compliance with the principle that the determination of corporate objectives and the related incentive programmes must be conducted in accordance with the principles of fairness and balance, by not identifying objectives that are overly ambitious and/or difficult to achieve through ordinary operations and that may induce undue conduct;
- where necessary, the establishment of a timetable regarding the maintenance of the regularity of the residence permit over time for non-EU staff employed on a permanent/permanent basis;
- the assignment of any company assets (e.g. cars, sim cards, telephones, tablets), through the use of special standard notices/forms for taking them over, signed for acceptance, and also containing the commitment to their correct use in compliance with the provisions of the Group, the Company and current legislation, providing, for new recruits, for the inclusion of such clauses in the relevant employment contract;
- the filing in paper/informatic format, by creating a file for each employee, of the data/documents/acts prepared in the course of the employment relationship (e.g. career progressions, assignment of bonuses, residence permits).

3.4. PROCUREMENT OF GOODS AND SERVICES AND CONSULTANCY

3.4.1. DESCRIPTION OF THE POTENTIAL RISK PROFILE

The procurement of goods, services and consultancy may theoretically entail the risk of committing the offences of:

- receiving stolen goods (Article 648 of the Criminal Code), in the event, for instance, of the purchase of goods from any crime, or in the event of the use by the supplier of resources of unlawful origin (e.g. plant and machinery for the performance of its business);
- terrorism and subversion of the democratic order (Article 25-quater of Legislative Decree 231/01) in the event that funds are directly or indirectly, but nevertheless voluntarily, provided in favour of persons intending to commit terrorist offences, through the selection and/or management of suppliers/subcontractors;
- culpable homicide (Article 589 of the Criminal Code) and culpable personal injury (Article 590, paragraph 3, of the Criminal Code), environmental offences (Article 25-undecies of Legislative Decree 231/01), offences of employment of third-country nationals whose stay is irregular (Article 25-duodecies of Legislative Decree 231/01), crimes against the individual (Article 25-quinquies of Legislative Decree 231/01) in the event that they are committed by suppliers/contractors within company areas and/or in any case under the control of the Company;
- criminal association (Article 416 of the Criminal Code) of a mafia type, including foreign ones (Article 416-bis of the Criminal Code), in the event that the Company uses suppliers/contractors referable to them;
- bribery among private individuals (Article 2635(3) of the Civil Code) and incitement to bribery among private individuals (Article 2635-bis(1) of the Civil Code), where the Company gives, offers or promises, even through an intermediary, a fee or other utility, to a supplier's salesperson in order to obtain an undue benefit/utility not due (e.g. off-market discount) or to the supplier's technician in order to prevent him from highlighting problems encountered in the performance of his activities;
- improper use and falsification of non-cash payment instruments (Article 493-ter of the Criminal Code), where a senior or subordinate person of the Company makes payments for the acquisition of goods and services by means of a payment card not registered in his name or other non-cash instrument, and, therefore, by means of improper use, in order to obtain an advantage for the Company from that transaction;
- fraudulent declaration by means of invoices or other documents for non-existent transactions (Article 25-quinquiesdecies of Legislative Decree 231/01 - Article 2, paragraphs 1 and 2-bis of Legislative Decree 74/00), fraudulent declaration by means of other devices (Article 25-quinquiesdecies of Legislative Decree 231/01 - Article 3 of Legislative Decree 74/00). These offences could, in fact, be committed in the abstract in the event that the Company, in order to evade taxes, uses fictitious passive invoices which alter the values of the annual declaration or employs fraudulent means aimed at obstructing the tax authorities' assessment;
- Self-laundering (Article 648-ter.1 of the Criminal Code), in the event that the Company, following the commission or complicity in the commission of one of the aforementioned offences, as well as of other offences referred to in Legislative Decree 231/01, obtains utilities which it employs, substitutes or transfers, in such a way as to concretely hinder the identification of their criminal origin.

The process of procurement of goods, services and consultancy could also in abstract terms be the instrument through which offences are committed:

- corruzione per l'esercizio della funzione (art. 318 c.p.), corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.), corruzione in atti giudiziari (art. 319-ter c.p.), corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), istigazione alla corruzione (art. 322 c.p.), embezzlement, extortion, undue inducement to give or promise benefits, bribery and incitement to bribery of members of international courts or bodies of the European Communities or international parliamentary

assemblies or international organisations and officials of the European Communities and foreign states (Article 322-bis of the criminal code);

- trafficking in unlawful influence (Article 25 of Legislative Decree 231/2001 - Article 346-bis of the criminal code);
- of undue inducement to give or promise benefits (Article 319-quater of the Criminal Code);
- extortion (Article 317 of the criminal code);
- inducement not to make statements or to make false statements to the judicial authorities (Article 377-bis of the criminal code).

These offences could, in fact, be committed in the abstract through non-transparent management of the supplier selection process. Therefore, the issuing of purchase orders may be instrumental in creating funds that can be used for corrupt purposes against public officials/public service employees or private individuals, for instance:

- in the case of the granting or promising of a fictitious contract in favour of a public official or a private individual (or of family members or persons or companies related to them or liked by them) in order to reward them for undue favours or to obtain an undue advantage;
- through the creation of funds as a result of contracted services at above-market prices, to be given or promised to public officials or private individuals, in order to obtain favours within the scope of the company's activities.

3.4.2. ACTIVITIES AT RISK AND ENTITIES INVOLVED

Below are the corporate bodies involved in the management of the activity at risk Procurement of goods, services and consultancy (Head of DI activities - Supply Chain - Procurement - Functions involved Country Leader, Sales Finance, Sales Team, Sales Operation, Global Services Operations, Professional Services, Global Delivery, Customer Support, Sales Finance, Order Management, Legal Business Partner, Marketing & Communication).

3.4.3. SPECIFIC CONTROL PROTOCOLS

The activities connected with this risk area must be managed in compliance with company/group procedures, which, in addition to incorporating the principles expressed in the Code of Ethics and Conduct, provide for

- the definition of the main activities as well as the roles and responsibilities of the Functions/Areas involved, ensuring at each stage a separation of tasks/roles. More specifically, the key elements are listed below:
 - with regard to the purchase request phase, it is envisaged:
 - appropriate formalisation, through the use of company information systems;
 - a proper check of the adequacy of expenditure against the budget;
 - during the selection and selection of supply offers:
 - checking, as a preventive measure, available information (including financial information) on supplier counterparties, partners and consultants, to ascertain their respectability and the legitimacy of their activities, before establishing business relations with them;
 - compliance with the principle that the selection of suppliers of goods, services and facilities must be based on objective, transparent and documentable evaluation criteria, in accordance with the principles of the Code of Ethics and Conduct;
 - at the order/contract stage must be provided for:

Special Part

- the definition of economic conditions consistent with the type of supply requested;
- signing of the supply order/contract by a person with a suitable power of attorney to that effect;
- the phase of receiving, checking and evaluating the supply and authorising payment must provide that
 - the receipt, as far as possible, of the goods is carried out by a party (the party requesting the supply) other than the party managing the offer and negotiation phase with the supplier and the party making payment for the supply/performance;
 - any critical issues or difficulties of any kind in the performance of contractual relations, including any non-performance or partial performance of contractual obligations, are highlighted in writing and handled by the competent Functions in accordance with the contractual agreements and in compliance with the law and other applicable regulations;
 - the activity performed by the supplier/consultant is duly documented and the Department that has used their services must, before the payment of the relevant fees, certify the actual performance;
 - outgoing financial flows are authorised according to the Company's powers of attorney and managed according to the defined process;
 - the continued fulfilment by suppliers of the requirements of reliability, correctness, professionalism and good repute must be monitored;
- the inclusion of suppliers in a 'Qualified Supplier List', after passing a trial period, the outcome of which must be formalised;
- the preparation of standard general terms and conditions of supply, which include, inter alia, the clause according to which any breach committed by the supplier (and ascertained by the Company and/or the competent authorities), with reference to Legislative Decree 231/01 or the Code of Ethics and Business Conduct, shall entail the possibility of termination of the contract, as well as legal recourse against the persons who committed such breach;
- adequate storage of relevant documentation, so as to ensure the traceability of the operations carried out.

3.5. CORPORATE AFFAIRS

3.5.1. DESCRIPTION OF THE POTENTIAL RISK PROFILE

The process of managing corporate affairs is potentially exposed to the risk of the following offences being committed (or concurred in):

- corruzione per l'esercizio della funzione (art. 318 c.p.), corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.), corruzione in atti giudiziari (art. 319-ter c.p.), corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), istigazione alla corruzione (art. 322 c.p.), embezzlement, extortion, undue inducement to give or promise benefits, bribery and incitement to bribery of members of international courts or bodies of the European Communities or of international parliamentary assemblies or international organisations and of officials of the European Communities and foreign states (Article 322-bis of the Criminal Code). 322-bis of the Criminal Code), as well as undue inducement to give or promise benefits (Article 319-quater of the Criminal Code) and inducement not to make statements or to make false statements to the judicial authorities (Article 377-bis of the Criminal Code), in view of the fact that managing corporate affairs involves systematic contacts and obligations towards PA officials (by way of example only: e.g. Notaries, Chamber of Commerce, Courts, Registry Offices, etc.). To this end, contact with public officials could represent an opportunity to offer money or other benefits to them in order to obtain favourable treatment, e.g. by inducing them to omit/mit the imposition of sanctions to be imposed as a result of irregularities revealed during inspections (for the analysis of the risk area relating to relations with the PA, see paragraph 3.11 of this Special Section);
- unlawful transactions on the company's shares or quotas or those of the parent company (Article 2628 of the Civil Code) and transactions to the detriment of creditors (Article 2629 of the Civil Code); this is in light of the fact that the activities of the corporate bodies may lead to board/assembly resolutions connected with capital transactions (such as, for example the purchase or subscription, outside the cases permitted by law, of shares or quotas, reductions in share capital or mergers with other companies or demergers in breach of Articles 2306, 2445 and 2503 of the Civil Code) which, potentially, may damage the integrity of the share capital and the rights of creditors;
- Unlawful influence on the shareholders' meeting (Article 2636 of the Civil Code). The offence is committed when, by simulated or fraudulent acts, a majority in the shareholders' meeting is determined in order to obtain an unfair profit for oneself or others; it is a 'common offence', which can therefore be committed by anyone. This offence may take the form of using unplaced shares, exercising voting rights under another name, or using other unlawful means;
- false corporate communications (Article 2621 of the Italian Civil Code), minor facts (Article 2621-bis of the Italian Civil Code), obstruction of control (Article 2625 of the Italian Civil Code), undue return of contributions (Article 2626 of the Italian Civil Code), unlawful distribution of profits and reserves (Article 2627 of the Italian Civil Code), fictitious capital formation (Article 2632 of the Italian Civil Code), undue distribution of corporate assets by liquidators (Article 2633 of the Italian Civil Code). The ways in which these offences can be committed include, for example, the concealment in whole or in part by fraudulent means of information/facts that should have been communicated to the Control Body concerning the Company's economic, asset or financial situation, or the falsification/omission of communications/requirements to the same.

3.5.2. ACTIVITIES AT RISK AND ENTITIES INVOLVED

Below are the corporate bodies involved in the management of the risk activity Corporate Business Management (Legal Business Partner - Functions involved Country Leader, Legal Business Partner, Sales Finance).

3.5.3. SPECIFIC CONTROL PROTOCOLS

In addition to the principles expressed in the Code of Ethics and Conduct, the Company provides that

- Recipients are required to observe a conduct aimed at ensuring the regular functioning of the Company, and the proper interaction between its corporate bodies, ensuring and facilitating all forms of control over the management of the company, in the manner provided for by law, as well as the free and regular formation of the will of the shareholders' meeting;
- it is forbidden to unlawfully determine or influence the passing of resolutions at the shareholders' meeting, by carrying out simulated or fraudulent acts to that end, which are intended to artificially alter the normal and correct procedure for the formation of the will of the shareholders' meeting;
- Recipients are required to ensure strict compliance with the provisions of the law protecting the integrity and effectiveness of the share capital, so as not to create damage to the guarantees of creditors and, more generally, to third parties;
- Activities connected with this area of risk must be managed in accordance with operational methods that ensure the segregation of duties and adequate traceability of operations;
- All operations on the Company's share capital, the allocation of profits and reserves, the purchase and sale of shareholdings and business units, mergers, demergers and spin-offs, as well as all operations that could potentially damage the integrity of the share capital must be inspired by the following principles:
 - transparency, fairness and compliance with regulations;
 - the assignment to the Board of Directors of the prior approval of corporate transactions that may have a significant impact on the company's profitability, assets and liabilities and financial position;
 - the assignment of decision-making and operational responsibilities for the aforementioned operations, as well as the coordination mechanisms between the various corporate Functions/Areas involved.

With reference to relations with the Control Body, the Company provides:

- the timely transmission to it of all documents relating to items on the agenda of meetings and Boards of Directors' meetings or on which the Statutory Auditor must express an opinion;
- the provision of documents on the management of the Company to enable it to carry out its audit activities;
- the provision of periodic meetings between the Control Body and the Supervisory Board to verify compliance with the company's rules and procedures on corporate law;
- how to archive and preserve the documentation produced.

3.6. ADMINISTRATION, FINANCE AND CONTROL

3.6.1. DESCRIPTION OF THE POTENTIAL RISK PROFILE

Activities related to budgeting, bookkeeping, budget preparation and taxation management have the following potential risk profiles:

- improper management of the same, impacting on the representation of the equity, economic and financial situation of the Company, could constitute one of the prerequisites for the commission or concurrence in the commission of the offences of false corporate communications (Article 2621), minor offences (Article 2621-bis of the Italian Civil Code), transactions to the detriment of creditors (Article 2629 of the Italian Civil Code) and fictitious capital formation (Article 2632 of the Italian Civil Code). These offences are committed by presenting material facts in the financial statements, reports or other corporate communications required by law, addressed to shareholders or the public, that are untrue and could mislead the recipients as to the economic, asset or financial situation of the company or the group to which it belongs, with the intention of deceiving shareholders, creditors or the public; or by omitting, with the same intention, material information on the same situation whose disclosure is required by law. Therefore, these offences could, in the abstract, occur, for instance, through:
 - the statement of material facts not corresponding to the truth;
 - the over- or under-valuation of estimated/valued balance sheet items;
 - the valuation that knowingly deviates from the statutory valuation criteria in a manner materially likely to mislead the recipients of the communications;
 - the modification of accounting data in the computer system;
 - the omission of information, the disclosure of which is required by law, concerning the economic, asset or financial situation of the company or the group to which it belongs, even where the information relates to assets owned or administered by the company on behalf of third parties, etc;
- fraud (Article 640(2)(1) of the Criminal Code). This offence could be committed through the preparation of untrue documentation in the preparation of tax returns, for instance by indicating untrue or non-existent aspects;
- fraudulent declaration through the use of invoices or other documents for non-existent transactions (Article 25-quinquiesdecies of Legislative Decree 231/01 - Article 2(1) and (2-bis) of Legislative Decree 74/2000). This offence could occur if, in order to evade taxes, the Company indicates fictitious passive elements in its income tax or value added tax declarations. Fictitious passive elements or assets lower than the real ones are indicated in the annual declaration by means of registered documents;
- fraudulent declaration by means of other artifices (Article 25-quinquiesdecies of Legislative Decree 231/01 - Article 3 of Legislative Decree 74/00). This offence could occur if the Company, in order to evade taxes and with the consciousness and will of exceeding the thresholds of punishability under the law, makes a false representation in the compulsory accounting records or employs fraudulent means capable of hindering the assessment by the tax authorities or submits an untrue declaration;
- issuing invoices or other documents for non-existent transactions (Article 25-quinquiesdecies of Legislative Decree 231/01 - Article 8, paragraphs 1 and 2-bis of Legislative Decree 74/00). This offence could be committed if, in order to allow a third party to evade income tax or value added tax, it issues invoices or other documents for operations never performed, in exchange for the recognition by the third party of an economic advantage for the Company such as, for example, the approval of an order variant by the Customer;
- Concealment or destruction of accounting documents (Article 25 quinquiesdecies of Legislative Decree 231/01 - Article 10 of Legislative Decree 74/00) This offence may occur where the

Company conceals or destroys accounting records or documents which must be kept, in order to make it impossible to reconstruct the Company's income and turnover;

- fraudulent evasion of tax payments (Article 25 quinquiesdecies of Legislative Decree 231/01 - Article 11 of Legislative Decree 74/00). This offence could be committed if the Company simultaneously performs fraudulent acts on its own assets in order to render ineffective, for itself or for others, even partially, the compulsory collection procedure, or if it indicates, in the documentation submitted for the purposes of the tax settlement procedure, assets or liabilities other than the real ones in order to obtain a lower payment of the total amount due;
- False declaration (Article 25 quinquiesdecies of Legislative Decree 231/01 - Article 4 of Legislative Decree 74/00). This offence could be committed in the event that, in order to evade value added tax in the cross-border system for a total amount of not less than EUR 10 million, in the annual declaration relating to the aforementioned tax, he indicates assets for an amount lower than the actual amount or non-existent liabilities;
- omitted declaration (Article 25 quinquiesdecies of Legislative Decree 231/01 - Article 5 of Legislative Decree 74/00). This offence could be committed in the event that, in order to evade value added tax in the cross-border system for a total amount of not less than 10 million, the Company does not submit, despite being obliged to do so, the annual declaration relating to the aforementioned tax;
- Undue compensation (Article 25 quinquiesdecies of Legislative Decree 231/01 - Article 10-quater of Legislative Decree 74/00). This offence could occur in the event that, in order to evade value added tax in the cross-border system for a total amount of not less than 10 million, the Company uses non-existent and/or not due credits in compensation.

Finally, the activities of this risk area may in abstract terms constitute conduct relating to receiving stolen goods (Article 648 of the Criminal Code), money laundering (Article 648-bis of the Criminal Code), the use of money, goods or benefits of unlawful origin (Article 648-ter of the Criminal Code), and self-laundering (Article 648-ter.1 of the Criminal Code). For example, the Company could incur the latter offence if, following the commission or complicity in the commission of a crime (among those provided for by Legislative Decree no. 231/01), it obtains utilities which it uses, substitutes or transfers, in such a way as to concretely hinder the identification of their criminal origin.

The process of procurement of goods, services and consultancy could, in the abstract, also be the instrument through which offences are committed:

- corruzione per l'esercizio della funzione (art. 318 c.p.), corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.), corruzione in atti giudiziari (art. 319-ter c.p.), corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), istigazione alla corruzione (art. 322 c.p.), embezzlement, extortion, undue inducement to give or promise benefits, bribery and incitement to bribery of members of international courts or bodies of the European Communities or international parliamentary assemblies or international organisations and officials of the European Communities and foreign states (Article 322-bis of the criminal code);
- trafficking in unlawful influence (Article 25 of Legislative Decree 231/2001 - Article 346-bis of the criminal code);
- of undue inducement to give or promise benefits (Article 319-quater of the Criminal Code);
- extortion (Article 317 of the criminal code);
- inducement not to make statements or to make false statements to the judicial authorities (Article 377-bis of the criminal code);
- bribery among private individuals (Article 2635(3) of the Civil Code) and incitement to bribery among private individuals (Article 2635-bis(1) of the Civil Code).

This is because this process can be instrumental in establishing hidden funds that can be used for corrupt purposes, for instance through

- the accounting of fictitious items (e.g. false invoices for non-existent services);
- failure to account for items;
- the overvaluation of assets of the Company.

3.6.2. ACTIVITIES AT RISK AND ENTITIES INVOLVED

The main activities to be considered abstractly at risk and the corporate bodies involved in their management are highlighted below:

- Preparation of budget and periodic analysis of deviations (Country Leader and Finance EMEA - Functions involved Sales Finance, Sales Operations);
- Receipt, verification and recording of supplier invoices (Hitachi Group Company - Finance EMEA - Functions involved Country Leader, Order Management, Sales Finance);
- Issuing of active invoices (Finance EMEA - Functions involved Country Leader, Sales Finance);
- Performing accounting entries (Finance EMEA - Functions involved Country Leader, Sales Finance, Legal Business Partner);
- Preparation of financial statements and tax returns (Head of Finance EMEA - Functions involved Country Leader).

3.6.3. SPECIFIC CONTROL PROTOCOLS

The activities connected with this risk area must be managed not only in accordance with the principles contained in the Code of Ethics and Code of Conduct, but also in compliance with the company/group procedures, which provide:

- with regard to reporting, the periodic preparation of a cost forecast and a sales budget in order to ensure the monitoring of company performance;
- with reference to the keeping of accounts, the preparation and approval of financial statements and other corporate communications of an administrative accounting nature, and the management of taxation:
 - carrying out verification and control activities on the correctness of the invoices issued (e.g. correct application of VAT, withholding tax) prior to their approval;
 - the issue of active invoices:
 - in manual mode, upon successful acceptance or issue of the service performance certificate by the Customer;
 - automatically by the information system when the order is closed in the system;
 - the preparation of periodic accounting statements;
 - a list of the data and information that each corporate function must provide to the responsible function, as well as the criteria for their processing and the timing of their delivery;
 - the transmission of data and information to the responsible function by computer, so as to trace the various steps and identify the persons entering the data into the system;
 - the traceability of accounting operations, for the preparation of the financial statements, with particular reference to those relating to assessment and adjustment entries or those involving the need to make estimates;

Special Part

- the timely transmission of the draft budget to all members of the Board of Directors and the Controlling Body, as well as an appropriate record of this transmission;
- the holding of at least annual joint meetings between the Country Leader, the Control Body and the Supervisory Board;
- Adequate filing and storage of administrative/accounting documents in compliance with civil and tax regulations, so as to ensure their immediate traceability.

3.7. FINANCIAL RESOURCES

3.7.1. DESCRIPTION OF THE POTENTIAL RISK PROFILE

The management of financial resources may theoretically entail the risk of committing the offences of:

- Receiving stolen goods (Article 648 of the Criminal Code), money laundering (Article 648-bis of the Criminal Code), use of money, goods or utilities of unlawful origin (Article 648-ter of the Criminal Code) and self-laundering (Article 648-ter1 of the Criminal Code) through the movement of financial flows connected with purchasing activities and activities relating to the sale of products/services (please refer to these activities for more details on the specific risk profile);
- criminal association and mafia-type association, including foreign ones (Articles 416 and 416-bis of the Criminal Code), in the event that, for example, the Company knowingly procures financial resources to be destined to persons associated with these types of associations;
- bribery among private individuals (Article 2635(3) of the Civil Code) and incitement to bribery among private individuals (Article 2635-bis(1) of the Civil Code), where, for example, a Company contact person gives/promises/offer undue remuneration (e.g. money or other benefits):
 - to the insurance company, in order to obtain better conditions and/or the granting of a guarantee that would not be given;
 - to the bank official, in order to obtain an advantage from a credit institution (e.g. better financing conditions, non-revocation of an overdraft facility in the face of non-compliance with covenants laid down in the conditions for obtaining the facility).

It should be noted that in the performance of certain activities (such as, for example, the management of subsidised loans), credit institutions are de facto and de jure equated with the Public Administration: in this case, there would be no offence of bribery between private individuals/conspiracy to bribery between private individuals, but those of bribery/conspiracy provided for in the context of offences against the Public Administration;

- undue use and falsification of non-cash payment instruments (Article 493 ter of the Criminal Code), in the event that a senior person or subordinate of HVI makes a payment or even a withdrawal by means of a payment card not in his name or other non-cash instrument (with specific reference to access to the data and credentials of third parties - external and internal - functional to the use of non-cash payment instruments), and therefore by means of undue use, in order to obtain an unlawful advantage for the Company from that transaction. The offence could also be committed in the event that a senior person or subordinate of HVI misappropriates the credentials and identification and banking data of a customer (e.g. identity card, IBAN, Tax Code) in order to open a payment system through which he receives payments in favour of the Company itself or through which he unduly makes payments to third parties (suppliers, consultants, etc.);
- fraudulent transfer of valuables (Article 512-bis of the Criminal Code), which may occur if an HVI representative makes fictitious registrations/transfers of assets and/or valuables in order to avoid their seizure/confiscation or to commit money laundering or selflaundering offences.

The management of financial flows constitutes one of the instrumental ways through which, in principle, offences could be committed:

- corruzione per l'esercizio della funzione (art. 318 c.p.), corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.), corruzione in atti giudiziari (art. 319-ter c.p.), corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), istigazione alla corruzione (art. 322 c.p.), embezzlement, extortion, undue inducement to give or promise benefits, bribery and incitement to bribery of members of international courts or bodies of the European Communities or international parliamentary assemblies or international organisations and officials of the European Communities and foreign states (Article 322-bis of the criminal code);
- inducement to give or promise benefits (Article 319-quater of the criminal code);

- trafficking in unlawful influence (Article 346-bis of the Criminal Code);
- fraud (Article 640(2)(1) of the Criminal Code).

These offences could, in fact, be committed in the abstract through a non-transparent and incorrect management of monetary and financial flows, which could lead to the establishment of 'availabilities' functional to the realisation of unlawful conduct, including, typically, corrupt conduct, for example through

- the misuse of corporate current accounts to make sums of money available or to make it difficult to trace movements of funds;
- making payments of fictitious invoices in order to create 'availability';
- the recognition of fictitious expense reimbursements or advances in whole or in part;
- the use of cash sums to create 'liquid assets';
- the creation of funds against false invoices, in whole or in part.

3.7.2. ACTIVITIES AT RISK AND ENTITIES INVOLVED

The main activities to be considered abstractly at risk and the corporate bodies involved in their management are highlighted below:

- Management of payments and collections (Head of Finance EMEA - Functions involved Country Leader, Sales Finance);
- Managing relations with credit and insurance institutions (Head of Finance EMEA - Functions involved Country Leader, Sales Finance).

3.7.3. SPECIFIC CONTROL PROTOCOLS

In addition to the principles expressed in the Code of Ethics and Conduct, the Company generally provides that

- any act of a financial nature of the Company must be authorised in advance by the competent offices, ensuring that it is in the Company's interest, that the cost is appropriate, that the sums disbursed are actually and fully intended for the Company, and must be arranged in accordance with the corporate powers conferred;
- payment by Customers must be made through the Customer's credit institution at which it is always possible to identify the person who arranged the transaction to the Company's credit institution, thus guaranteeing the possibility of tracing the person who arranged the transaction;
- payments must be made by bank transfer to current accounts in the name of the same person to whom the order/assignment is made (opened with credit institutions in the country of residence/registered office of the person to whom the order/assignment is made);
- Payments to numbered accounts or accounts for which the identity of the account holder cannot be precisely identified are prohibited;
- it is forbidden to have relations with parties based or otherwise operating in countries that do not guarantee corporate transparency;
- it is prohibited to carry out operations that prevent the reconstruction of the financial flow or make it less easy, such as, for example, fractional payments/disbursements made for that purpose.

It is also expected:

- with regard to payments of passive invoices, the obligation to:

Special Part

- carry out, prior to the execution of payments, a control and evaluation of the supply/performance by the requesting function;
- check the correspondence between what has been authorised and the relevant reference documents (contract/purchase order, coupons, F24, Expense Note, etc.);
- with reference to collection management and debt collection policy:
 - the granting of credit lines to customers, based on defined criteria, duly formalised and authorised by persons delegated to do so;
 - the definition of operating methods, information flows, tools and responsibilities with regard to monitoring overdue credit and reminders to the customer, ensuring adequate segregation and traceability of activities;
- that the decision to open current accounts rests with Headquarters, also taking into account the identified needs and requirements of the individual local companies;
- the definition of appropriate filing and storage methods for the documentation produced, so as to ensure its traceability.

3.8. INFORMATION SYSTEMS

3.8.1. DESCRIPTION OF THE POTENTIAL RISK PROFILE

The management of information systems may in abstract terms lead to the commission of offences:

- computer fraud to the detriment of the State or other public body (Article 640-ter(1) of the Criminal Code);
- of computer crimes and unlawful data processing (Article 24-bis of Legislative Decree 231/01), set out below:
 - falsification of a public electronic document with evidentiary effect (491-bis of the criminal code);
 - Unauthorised access to a computer or telecommunications system (615-ter of the criminal code);
 - Unauthorised possession, dissemination and installation of equipment, codes or other means of accessing computer or telecommunications systems (Article 615-quater of the criminal code);
 - Unlawful possession, dissemination and installation of computer equipment, devices or programmes intended to damage or interrupt a computer or telecommunications system (Article 615-quinquies of the criminal code);
 - unlawful interception, obstruction or interruption of computer or telematic communications (Article 617-quater of the criminal code);
 - Unlawful possession, dissemination and installation of equipment and other means of intercepting, impeding or interrupting computer or telematic communications (Article 617-quinquies of the criminal code);
 - damaging computer information, data and programmes (635-bis of the criminal code);
 - damage to computer information, data and programmes used by the State or other public body or in any case of public utility (635-ter of the Criminal Code);
 - damaging computer or telecommunications systems (635-quater of the criminal code);
 - damaging computer or telecommunications systems of public utility (635-quinquies of the criminal code);
- possession and dissemination of computer equipment, devices or programmes aimed at committing offences involving non-cash payment instruments (493 quater of the Criminal Code) and computer fraud aggravated by the carrying out of a transfer of money, monetary value or virtual currency (640 ter paragraph 2 of the Criminal Code) respectively in the hypothesis that
 - a senior person or subordinate of HVI unduly possesses computer programs or software specifically designed to carry out unlawful fund transfer operations, with the intention of procuring an economic advantage for the Company;
 - a senior person or subordinate of HVI, using an access code not assigned to him or ICT resources not assigned to him, illegally penetrates the bank computer system (e.g. home banking) and carries out unlawful fund transfer transactions in order to conceal their unlawful origin and procure an advantage to the Company
- some of those covered by Article 25-novies (offences relating to violation of copyright), including those listed below:
 - Unauthorised making available to the public, in a system of telematic networks, through connections of any kind, of a protected intellectual work or part thereof;
 - Unauthorised duplication, for profit, of computer programmes;

- import, distribution, sale or possession for commercial or business purposes or rental of programmes contained in media not marked by the SIAE;
- Providing means to remove or circumvent computer program protection devices;
- reproduction, transfer to another medium, distribution, communication, presentation or demonstration in public, of the contents of a database; extraction or re-use of the database; distribution, sale or rental of databases.

The information systems management process constitutes, in principle, a tool through which some of the offences of the types set out in Legislative Decree 231/01 may be committed, including the offences of

- false corporate communications (Article 2621 of the Civil Code) and minor facts (Article 2621-bis of the Civil Code);
- impeded control (Article 2625 of the Civil Code);
- fraud (Article 640(2)(1) of the Criminal Code);
- trafficking in unlawful influence (Article 346-bis of the Criminal Code);
- corruzione per l'esercizio della funzione (art. 318 c.p.), corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.), corruzione in atti giudiziari (art. 319-ter c.p.), induzione indebita a dare o promettere utilità (art. 319-quater c.p.), corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), istigazione alla corruzione (art. 322 c.p.), embezzlement, extortion, undue induction to give or promise benefits, bribery and incitement to bribery of members of international courts or bodies of the European Communities or of international parliamentary assemblies or international organisations and of officials of the European Communities and of foreign states (Article 322-bis of the criminal code) and undue induction to give or promise benefits (Article 319-quater of the criminal code);
- inducement not to make statements or to make false statements to the judicial authorities (Article 377-bis of the criminal code);
- bribery among private individuals (Article 2635(1) of the Civil Code) and incitement to bribery among private individuals (Article 2635-bis(3) of the Civil Code).

The offences listed above could be committed, for instance, through abnormal management:

- of systems security, which could allow access, alteration and/or deletion of data and information intended for the Public Administration, third-party stakeholders or, in any case, the outside world;
- of system changes, which could allow unauthorised changes to be made to the system and/or information, data and computer programmes to be damaged/deleted;
- backups/restore, which could allow unauthorised access and/or modification to data and loss of information, data and computer programmes, preventing or hindering the performance of control activities.

3.8.2. ACTIVITIES AT RISK AND ENTITIES INVOLVED

It is noted below that the risk activity Information Systems Management is managed by the parent company.

It should be noted that Hitachi Vantara Italia employees who routinely use computer systems consequently have ample opportunity to access computer and telematic tools and data in the context of their ordinary work activities. For this reason, given the widespread diffusion at the Company of computer systems and tools, with regard to computer crimes and unlawful processing of data covered by Article 24-bis, it is considered that the risk of their commission is diffuse and not localised, since they could abstractly be committed in each sensitive activity of the various Functions.

3.8.3. SPECIFIC CONTROL PROTOCOLS

The activities connected with this risk area must be managed in compliance with the principles contained in the Code of Ethics and Conduct and the company/group procedures, which define the information flows, instruments and responsibilities, with regard to

- the management of ICT risks, enabling the assessment of ICT risks and the preparation of Action Plans for their management;
- ICT security management, with reference to activities:
 - backups of data and programmes, providing for the performance of retention activities and defining the processing cadences of backups;
 - related to the management of security, system protection, data integrity and confidentiality.

In particular, the following aspects are illustrated:

- the guidelines for the allocation of identifiers and access rights, in compliance with information needs, the corporate role and in accordance with the principle of Segregation of Duties (SOD), to users, ICT personnel and third parties, under which, inter alia, the following is provided:
 - the identification, authentication and enabling of access to the applications, infrastructure and network by assigning personal identification codes ('user' and 'password') to each resource (personnel or third parties), and the implementation of appropriate mechanisms for the secure exchange of information via e-mail and the Internet;
 - the adoption by each resource of appropriate measures to ensure the secrecy of its access credentials, and the prohibition to disclose or make them known to others;
 - the attribution of credentials that do not contain references that can be easily traced back to the data subject and the definition of the frequency with which credentials must be renewed, also depending on the sensitivity of the data processed;
 - the duty of each resource not to leave his or her computer workstation unattended or accessible at the end of working hours, during work breaks, or during meetings away from his or her workstation;
 - the request for and granting of access privileges to the various company systems in compliance with a (SOD) principle and according to the tasks performed, as well as the periodic control of the same with modification and/or removal of those that no longer comply with the evolution of the company situation;
- monitoring systems to detect the presence of viruses, other malicious software, devices and software that do not comply with company standards and/or are unauthorised, and providing for the removal of irregular devices and software and/or their regularisation, in order to restore the security situation of the systems;
- appropriate protection systems for the use of devices both inside and outside the company premises (e.g. encryption and automatic data backup systems for PCs; encryption systems and use of special applications for mobile phones);
- ICT demand management, i.e. the management of user requests (in particular, HW and SW equipment, Internet connections, e-mail provisioning, application/infrastructure maintenance) and therefore the regulation of request, assessment and authorisation, take-over, delivery and closure activities, with the related operational and authorisation responsibilities;
- the management of ICT assets, from the phase of their acquisition to that of their disposal, also regulating the activities of assignment, redelivery, disposal with constant updating and periodic reconciliation of the inventory;

- the collection of ICT initiatives, to be understood as the collection of ICT needs (applications, infrastructures), their evaluation and approval in compliance with the ICT strategic/operational plan and the corporate budget;
- the management of application and infrastructure changes, and the assignment of operational/authorisation responsibilities in the routine and evolutionary maintenance phases (applications and infrastructure), ensuring adequate segregation of environments (development, testing, production);
- access to the CED premises. In particular, the criteria and procedures for issuing authorisations to access these premises are defined. In this regard, provision is made:
 - the assignment by the Corporate of company badges enabled according to the role played at the Company (with restricted access, with access to specific areas, etc.);
 - different access authorisation / badge allocation processes, depending on the requesting users (e.g. employee, visitor, supplier or intern) and as required;
- the management of site security by providing:
 - an activity to identify potentially critical areas;
 - a video surveillance system managed directly and uniquely by Corporate;
 - the allocation of time-restricted badges for the access of suppliers involved in the maintenance of the premises (e.g. cleaning company).

Furthermore, the Company (through the competent group structure) guarantees:

- the preparation and maintenance of the Disaster Recovery Plan;
- a careful analysis aimed at defining system profiles, in particular for those systems that impact financial reporting or that contain confidential, sensitive or particularly critical data for the Company, defining standard profiles on the basis of company positions, in compliance with SOD incompatibilities;
- the formalisation of system administrator appointments;
- the signing by third parties who are given access to the network managed by the Company, of a declaration in which they undertake to use it in compliance with the law and the Code of Ethics and Conduct;
- systems to block access to unauthorised websites;
- the regulation of the opening and use of the PEC, providing in particular for the signing by the resource(s) who access(es) the same and who do not have/do not have powers of representation for the Company of a declaration of commitment and use according to the indications received from the authorised attorney;
- periodic monitoring activities by means of:
 - the aggregate verification of system and application logs, so as to promptly identify activities that do not comply with company rules;
 - monitoring the network for access and transmission of data that does not comply with company rules;
 - verification of so-called '*generic*' accounts (non-named users), for:
 - check that accounts are uniquely assigned and therefore always traceable to a specific user;
 - provide for the modification and/or removal of those no longer in conformity with the evolution of the company's situation;

- the provision of continuous distance training by the Corporate to personnel on the correct behaviour to be adopted in the use of mobile phones and any other company devices, as well as awareness-raising activities through the holding of information/training meetings aimed at personnel.

It should also be noted that:

- all processing operations must be carried out in such a way as to ensure compliance with security measures, the utmost confidentiality of the information coming into its possession, considering all data confidential and, as a rule, subject to official secrecy;
- the individual work steps and the conduct to be observed must make it possible to prevent data from being subject to the risk of loss or destruction, from being accessed by unauthorised persons, from being processed in a way that is not permitted or not in accordance with the purposes for which the data were collected;
- the workstation must be:
 - used only for work-related purposes;
 - used exclusively by a single user;
 - protected, preventing third parties from accessing the data without authorisation;
- is the duty of the employee:
 - not use private IT resources (PCs, peripherals, tokens, etc.) in the company;
 - do not install any software on workstations or company laptops/devices;
 - do not leave confidential information on your desk in whatever medium it is stored;
 - ;
- telematic communication tools (Internet and e-mail) must be used solely and exclusively for work purposes. Behaviour that may cause damage to the Company is forbidden. In particular, the user shall observe the following rules:
 - Internet surfing is permitted only on sites relevant and necessary for the performance of the assigned tasks;
 - It is not permitted to download free software (freeware or shareware) from Internet sites;
 - you may not register on Internet sites or participate in discussion forums if this is not strictly necessary for the performance of your work;
 - It is forbidden to open e-mails and file attachments of unknown origin or which present anomalous aspects;
 - it is not permitted to reply to messages from an unknown or doubtful sender as such an act assures the sender of the existence of the recipient;
 - The use of e-mail to communicate confidential information, personal data or critical data, without ensuring appropriate protection, is prohibited;
 - only the use of the programmes officially installed by the corporate information systems is permitted;
 - independent installation of programmes is prohibited;
 - it is forbidden to change the characteristics set on the equipment or to install storage, communication or other devices (e.g. burners, modems, wi-fi, etc.), to connect any equipment (e.g. switches, hubs, network storage devices, etc.) to the company network, to make connections to the outside world of any kind (e.g. via modem) using a PC that is simultaneously connected to the company network;

- an obligation is placed on all those who have received company computer equipment/devices to promptly report to the competent Function any theft, damage, loss, use or abnormal operation of such equipment/devices;
- it is prohibited to:
 - transfer outside the Company electronic files and any confidential documentation belonging to the Company;
 - use passwords of other corporate users;
 - use software and/or hardware tools designed to intercept, falsify, alter or suppress the content of computer communications and/or documents;
 - carrying out personal transactions, on one's own behalf or on behalf of third parties, including through an intermediary, using confidential information acquired in the course of one's duties, as well as the prohibition to recommend or induce others to carry out transactions using the aforementioned information;
 - downloading or sharing copyrighted material online without the specific approval of the owner.

3.9. HEALTH AND SAFETY AT WORK

3.9.1. DESCRIPTION OF THE POTENTIAL RISK PROFILE

In addition to a direct risk profile for offences of bribery, trafficking in unlawful influence, fraud and undue inducement to give or promise benefits (for the ways in which offences can be committed, see section 3.12 Relations with Public Institutions and Bodies) and the employment of third-country nationals whose stay is irregular (for the ways in which offences can be committed, see section 3.3. Acquisition, progression and management of personnel), a direct risk profile insofar as they could give rise to offences referred to in the cases provided for by Legislative Decree 231/01 Article 25 septies, concerning safety at work, namely manslaughter and serious or very serious injuries committed in violation of the rules, in the event of accidents at work.

3.9.2. ACTIVITIES AT RISK AND ENTITIES INVOLVED

The Risk Assessment Documents pursuant to Legislative Decree 81/08 contain the assessment of all risks to the safety and health of workers present in the workplace and an indication of the prevention and protection measures implemented as a result of the assessment.

Without prejudice to the identification and assessment of the risks referred to in the Risk Assessment Documents drawn up pursuant to Legislative Decree 81/08, as amended and supplemented, we set out below the main activities identified by the Company as potentially at risk for the commission of the offences referred to in Legislative Decree 231/01 Article 25-septies, together with the Functions involved:

- management of delegations of responsibility and appointments/designations of safety-relevant functions (by the Employer or his delegate within the limits of the powers conferred);
- management of the maintenance of general facilities and infrastructures in compliance with technical and structural standards and monitoring and control of physical, chemical and biological agents in the workplace (Regional Facilities Manager with the cooperation of the Employer's Delegates, within the limits of the powers conferred, and with the support of the RSPP);
- risk assessment and preparation of prevention and protection measures (Employer with the collaboration of the RSPP, RLS, Competent Doctor);
- management of emergencies and first aid and related periodic tests (Employer or his delegate, within the limits of the powers conferred, with the collaboration of the RSPP and the emergency and first aid team);
- management of contracts, works or supply contracts and safety at temporary or mobile construction sites (Employer or his delegate, within the limits of the powers conferred);
- management of periodic safety meetings and consultation of the RLS (Employer or his delegate, within the limits of the powers conferred, with the cooperation of the RSPP, the RLS and the Competent Doctor);
- management of occupational health and safety education, information and training (Employer with the support of Facilities EMEA and the collaboration of the RSPP);
- management of health surveillance and accidents (Employer and Competent Doctor with the collaboration of Facilities EMEA);
- acquisition of documentation and certifications required by law (Employer or his delegate, within the limits of the powers conferred, with the cooperation of the various Functions/Areas of the Company, each within the scope of its responsibilities and competences and the support of the RSPP);
- supervision and periodic checks on compliance with safe working procedures and instructions and on the effectiveness of the procedures adopted (Employer Managers and Supervisors with the cooperation of the RSPP).

3.9.3. SPECIFIC CONTROL PROTOCOLS

The activities associated with this risk profile must be managed in compliance with the general principles of conduct expressed in this Model, in the Code of Ethics and Code of Conduct, and in compliance with company procedures, which provide for the following

- management of delegated responsibilities and appointments/designations of safety-relevant functions. For the management of occupational health and safety issues, the Company has defined a system of powers and proxies adequate for the performance of sensitive activities and consistent with the organisational structure of the Company. In particular:
 - Appointments and designations of persons responsible for security matters are appropriately formalised and publicised within the Company;
 - verification of the possession and maintenance of the required competence and professionalism requirements for safety-relevant figures is ensured;
 - the resources entrusted with safety-relevant tasks are endowed with powers of organisation, management and control, and, where appropriate, of expenditure, appropriate to the structure and size of the organisation and the nature of the tasks assigned.

With particular reference to the delegation of functions by the Employer, as provided for in Article 16 of Legislative Decree 81/2008 as amended and supplemented, where not expressly excluded, it is permitted in compliance with the following principles of case law:

- effectiveness - existence and coexistence of decision-making and financial autonomy of the delegate;
 - technical and professional suitability and experience of the delegate;
 - supervision of the delegate's activity, non acquiescence, non-interference;
 - certainty, specificity and awareness;
- Management of the maintenance of general installations and infrastructure in compliance with technical-structural standards and monitoring and control of physical, chemical and biological agents in the workplace. This management includes:
 - the identification of and compliance with legal technical and structural standards concerning applicable equipment, facilities, workplaces, chemical, physical and biological agents;
 - formalising the contractual aspects governing the occupation of company premises by ensuring the clear allocation of responsibilities for the management of ordinary and extraordinary maintenance of general facilities and installations;
 - planning and management of ordinary and extraordinary, scheduled and breakdown maintenance of safety devices, equipment, machines and installations;
 - Verification and periodic inspection of equipment, facilities, workplaces, chemical, physical and biological agents in compliance with applicable regulations through public or private approved bodies.

Appropriate information flows are also envisaged between the SPP service and the Functions involved in the procurement process to ensure a preliminary assessment of the risks that may be introduced into the Company during procurement;

- Risk assessment and preparation of prevention and protection measures. With reference to this assessment, provision is made:
 - the assessment of workers' health and safety risks, including fire risks and those concerning groups of workers exposed to particular risks, including those related to work-related stress, those related to the use of company cars or deriving from off-site activities, those concerning pregnant workers, as well as those related to gender differences, age, origin from other countries and those related to the specific type of contract through which the work is

- performed. This assessment shall be carried out according to the methods and contents provided for in Articles 28 and 29 of Legislative Decree 81/08, as amended;
- the periodic updating of the risk assessment according to the methods provided for in Articles 28 and 29 of Legislative Decree 81/08 as amended;
 - the drafting, following the assessment referred to in the previous points, of Risk Assessment Documents (DVR) containing the contents set forth in Article 28 c. 2 of Legislative Decree 81/08, as amended and supplemented, in compliance with the indications provided by the specific rules on risk assessment contained in the subsequent titles of the aforementioned Decree;
- Emergency management and first aid and related periodic testing. With reference to this aspect, provision is made:
 - the designation and training of workers in charge of implementing fire prevention and firefighting measures, evacuation of workplaces in the event of serious and immediate danger, rescue, first aid and, in any case, emergency management. The number of designated emergency workers is defined in consideration of the organisational and operational structure of the Company and of the possible absences of those in charge due to holidays/illness/other ;
 - Identifying possible emergencies and planning how to deal with them, organising the necessary relations with the relevant public services and formalising procedures so that workers can cease their activities, or make themselves safe, by leaving the workplace;
 - informing workers and external personnel of the measures taken and the behaviour to adopt in the event of an emergency;
 - the planning and execution of periodic emergency and evacuation tests in accordance with the periodicity required by the regulations;
 - the availability of appropriate first aid and extinguishing equipment appropriate to the class of fire and level of risk present in the workplace, also taking into account the particular conditions in which they may be used;
 - the presence of plans showing escape routes and the location of fire-fighting and first aid facilities;
 - Management of contracts, works or supply contracts and safety at temporary or mobile construction sites. With reference to this aspect, it is envisaged:
 - management of contract or work or supply contracts and related interference risks in accordance with the provisions of Article 26 of Legislative Decree 81/08 as amended and Title IV of the aforementioned decree (temporary or mobile construction sites), where applicable;
 - the indication, in individual subcontracts, tenders and supply contracts, of the costs of the measures taken to eliminate or, where this is not possible, minimise occupational health and safety risks arising from interference of work;
 - the communication to the contractors of the relevant procedures and, if necessary, the name of the contact person for the contracted activity, as well as the inclusion of the disciplinary provisions relating to occupational health and safety in the contractual regulations between the parties;
 - Management of regular safety meetings and consultation of Workers' Safety Representatives (RLS). With reference to this aspect:
 - consultation of the RLS in all cases provided for in Article 50 of Legislative Decree 81/08, leaving adequate traceability;

- the execution, at least once a year, of a meeting attended by the Employer or his representative, the RSPP, the Competent Doctor, the RLS. During the meeting, of which adequate records are kept, at least the following topics are discussed:
 - o risk assessment document;
 - o trends in accidents, occupational diseases and health surveillance;
 - o selection criteria, technical characteristics and effectiveness of personal protective equipment;
 - o occupational health and safety information and training programmes.
- Management of education, information and training on health and safety at work. With reference to this aspect:
 - adequate education, information, training of workers in accordance with the provisions of Articles 36 and 37 of Legislative Decree 81/08 as amended and the State-Regions Agreements;
 - the possession of the necessary requirements by the safety trainers in accordance with the regulations in force;
 - periodic verification of learning.

The possible presence of posted or seconded workers must be taken into account when planning education, information and training activities.

- Management of health surveillance and accident management. With reference to this aspect
 - the preparation of the health protocol and its updating in relation to the evolution of the organisation;
 - the medical examination:
 - o preventive and periodic checks to establish the absence of contraindications to the work for which the worker is intended, in order to assess his suitability for the specific task;
 - o prior to resuming work, following absence for health reasons lasting more than sixty continuous days, in order to verify suitability for the job;
 - o in other cases provided for in the regulations in force.

Medical examinations for health surveillance cannot be carried out to ascertain states of pregnancy and in other cases prohibited by current legislation;

 - supervision of the fulfilment of the obligations laid down for the Competent Doctor with particular reference to carrying out annual inspections of workplaces and the submission of the annual report on the collective anonymous data of health surveillance;
 - the fulfilment of registration and reporting obligations in the event of accidents;
 - accident analysis and monitoring.

- Acquisition of documentation and certifications required by law. With reference to this aspect, provision is made for the identification of operating procedures aimed at ensuring the identification, acquisition and adequate storage of the documentation, records and certifications required by law, or that the Company deems necessary to certify compliance with the technical-structural standards laid down by law and an effective management of health and safety at work, by the various corporate Functions, each within the scope of its own responsibilities and competences;
- Supervision and periodic checks on compliance with safe working procedures and instructions and on the effectiveness of the procedures adopted. With reference to this aspect, provision is made:

Special Part

- monitoring compliance with safety procedures and instructions by company and external personnel and reporting any risks and discrepancies detected;
- the implementation of regular and systematic audits of the application and effectiveness of the procedures adopted;
- the definition and implementation of appropriate action plans to rectify any discrepancies and/or deficiencies found during the audits.

3.10. ENVIRONMENTAL ISSUES

3.10.1. DESCRIPTION OF THE POTENTIAL RISK PROFILE

The environmental aspects linked to the Company's activities present, in addition to a direct risk profile for offences of corruption, fraud, trafficking in unlawful influence and undue induction to give or promise benefits (for which please refer to paragraph 3.12 Relations with Institutions and Public Bodies), a direct risk profile in that, in the event of non-compliant management with the applicable legislative provisions on the environment, offences could arise, as provided for by Legislative Decree 231/01 art. 25 undecies.

The types of offences identified by the Company as potentially applicable are:

- Collection, transport, recovery, disposal, trade and intermediation of waste in the absence of or in breach of the prescribed authorisation, registration or communication (Article 256 c. 1 and 4 of Legislative Decree 152/06). The offence may be deemed to be abstractly committed in the event of complicity in the commission of the offence in the case of entrusting waste transport or disposal activities to unauthorised third party operators or operators operating in breach of authorisations and applicable legislation;
- illicit trafficking in waste (Article 259(1) Legislative Decree 152/06). The offence could be committed in the case of cross-border shipment of waste contrary to the provisions of the sectoral legislation, for example in relation to the shipment of waste mistakenly considered as 'technical material';
- activities organised for the illegal trafficking of waste (Article 260 c. 1 of Legislative Decree 152/06 - Repealed by Article 7 of Legislative Decree 21/18 and inserted in Article 452-quaterdecies of the Criminal Code). The offence could be committed if waste transport or disposal activities are entrusted to unauthorised third-party operators or operators operating in breach of authorisations and applicable legislation;
- culpable offences against the environment (452 quinquies of the criminal code). The offence could occur in the case of a fire in relation to the potential environmental consequences;
- criminal conspiracy and mafia-type conspiracy aimed, exclusively or concurrently, at committing one of the offences set out in Title vi-bis of the Penal Code and mafia-type conspiracy aimed at acquiring the management or control of economic activities, concessions, authorisations, contracts or public services in environmental matters (Article 452 octies of the Penal Code). The offence could be committed if the results of environmental supervisory and control activities are prevented or compromised by control authorities.

3.10.2. ACTIVITIES AT RISK AND ENTITIES INVOLVED

Below are the main activities identified by the Company as potentially at risk for the commission of environmental offences, together with the Functions involved:

- waste management (Regional Facility Manager);
- emergency prevention and management (Employer/Country Leader or his delegate, within the limits of the powers conferred, with the cooperation of the RSPP and the emergency and first aid team).

3.10.3. SPECIFIC CONTROL PROTOCOLS

For the management of environmental issues, the Company has defined a system of powers and proxies adequate for the performance of sensitive activities and consistent with the organisational structure of the Company itself. In particular, compliance with the following principles of jurisprudential elaboration is guaranteed:

- effectiveness - existence and coexistence of decision-making and financial autonomy of the delegate;
- technical and professional suitability and experience of the delegate;

- supervision of the delegate's activity, non acquiescence, non-interference;
- certainty, specificity and awareness.

The activities associated with this risk profile must be managed in compliance with the general principles of conduct expressed in this Model, in the Code of Ethics and Code of Conduct, and in compliance with company procedures, which provide for the following

- waste management:
 - compliance with the legal requirements for the waste producer, including the correct classification of waste by assigning the EWC code and compliance with the waste assimilation criteria established by the municipality of reference of each business unit;
 - discrimination between what is subject to waste regulation and what can be considered 'technical material' to be exempt from waste regulation;
 - the keeping of the loading/unloading register in case of production of special hazardous waste;
 - the transport and disposal of special waste in compliance with applicable legislation with particular reference to
 - entrusting special waste to authorised brokers, transporters and disposers;
 - verification of the correctness and completeness of the transport documentation (Waste Identification Form) of the waste;
 - monitoring of the documentation proving correct waste disposal (e.g. 4th copy of the Waste Identification Form), as well as taking legal measures in the event of failure to return the waste within the timeframe stipulated by the regulations;
 - the inclusion, in the contractual documents with contractors or subcontractors operating at the business units, of the obligations and prohibitions imposed on them in relation to the management of the waste they produce.

In the context of waste management, it is prohibited to

- mixing hazardous waste with non-hazardous waste and hazardous waste with different hazardous characteristics;
- perform own-account transport of waste;
- carry out transboundary shipments of waste or, where necessary, carry out such shipments in compliance with applicable legislation;
- Emergency prevention and management:
 - Identification of the types of emergencies that may cause damage to the environment and provision of appropriate technical and organisational measures to prevent emergencies and mitigate their effects.

With reference to this risk activity, the company procedures also regulate:

- the way in which supporting documentation and control activities carried out are archived and stored;
- monitoring compliance with environmental procedures and instructions by company and external personnel and reporting any discrepancies found;
- regular and systematic checks on the application and effectiveness of the procedures adopted;
- definition and implementation of appropriate action plans to rectify any discrepancies and/or deficiencies found.

Furthermore, it is forbidden to prevent, hinder, circumvent or compromise the results of environmental supervision and control activities, whether carried out on behalf of the Company or by control authorities.

3.11. PRE-LITIGATION AND LITIGATION MANAGEMENT

3.11.1. DESCRIPTION OF THE POTENTIAL RISK PROFILE

The activity of managing pre-litigation and litigation of whatever nature, i.e. civil, criminal, labour law, with the financial administration, etc., is potentially exposed to the risk of commission of the offences of:

- inducement not to make statements or to make false statements to the judicial authorities (Article 25-decies of Legislative Decree 231/01 - Article 377-bis of the criminal code). As regards the purposes and methods of commission of the unlawful conduct, these are identified in the abstract through:
 - the offer or promise of money or other benefits to a person called upon to make, before a judicial authority, statements usable in judicial proceedings;
 - acts of violence or threats of violence against a person called upon to make, before a judicial authority, statements that may be used in judicial proceedings;
- corruption in judicial proceedings (Article 25 of Legislative Decree 231/01 - Article 319-ter of the criminal code) and incitement to corruption (Article 25 of Legislative Decree 231/01 - Article 322 of the criminal code);
- fraud (Article 24 Legislative Decree 231/01 - Article 640(2)(1) of the Criminal Code);
- Undue inducement to give or promise benefits (Article 25 of Legislative Decree 231/01 - Article 319-quater of the criminal code);
- trafficking in unlawful influence (Article 346-bis of the Criminal Code);
- abuse of office (Article 25 of Legislative Decree 231/01 - Article 323 of the Criminal Code). This offence could be committed in the abstract in the event that, in a possible case with the European Union for the application of sanctions against which the Company lodges an appeal with the Court of the European Union, the Company persuades one or more judges to act by virtue of their office, for example by accepting an appeal that has reached the end of its term, thereby procuring a financial advantage for the Company and offending the financial interests of the EU;
- bribery among private individuals (Article 25-ter of Legislative Decree 231/01 - Article 2635, paragraph 3 of the Italian Civil Code) and incitement to bribery among private individuals (Article 25-ter of Legislative Decree 231/01 - 2635 bis of the Italian Civil Code);
- Self-laundering (Article 25-octies of Legislative Decree 231/01 - Article 648-ter 1 of the criminal code).

3.11.2. ACTIVITIES AT RISK AND ENTITIES INVOLVED

Below are the corporate bodies involved in the management of risk activity Pre-litigation and litigation management (Legal Business Partner - Functions involved Country Leader, Sales Finance).

3.11.3. SPECIFIC CONTROL PROTOCOLS

The activities connected with this risk area must be managed in compliance with the general principles of conduct expressed in this Model, in the Code of Ethics and Code of Conduct and in compliance with the company/group procedures, which provide for the following

- the definition of the strategy to be followed in litigation management;
- the traceability of litigation management activities and decisions on strategies adopted through:
 - the preparation by the litigation function of a specific report summarising the essential elements of the pending litigation;

- the preparation by Legal Business Partners or the sending to Legal Business Partners by the competent Functions of periodic "Reports" containing:
 - o the 'status' of existing or possible litigation;
 - o a brief description of them and of the possible litigation scenarios that could arise between the Company and third parties (e.g. partners, customers, etc.);
- the management of relations with the judicial authorities exclusively by the competent Functions/Areas;
- the choice of lawyers on the basis of criteria of professionalism and competence;
- the signing by the lawyer of a declaration of absence of conflicts of interest and acceptance of the Company's Code of Ethics and Business Conduct;
- the formalisation of settlement agreements;
- the payment of fees to external lawyers, on the basis of a description of the activities carried out, which allows the conformity of the fee to the value of the service rendered to be assessed, and subject to certification of the effectiveness of the service by the Function/Area that has availed itself of their services.

Reference is also made to the risk area Relations with public institutions and bodies for a description of the specific control protocols in the management of activities involving a relationship with a representative of the Public Administration.

3.12. RELATIONS WITH INSTITUTIONS AND PUBLIC BODIES

3.12.1. DESCRIPTION OF THE POTENTIAL RISK PROFILE

Before analysing the potential risk profile with regard to relations with public institutions and bodies, it should be noted that, for the definition of public official and person in charge of a public service, **Articles 357, 358 and 322-bis of the Criminal Code** are taken as reference for the preparation of this Model. In particular, the aforementioned articles set out the notion of Italian *public officials* and *persons in charge of a public service*:

1. persons performing a legislative or administrative public function, such as, for example:
 - parliamentarians and members of the government;
 - regional and provincial councillors;
 - MEPs and members of the Council of Europe;
 - persons performing ancillary functions (persons in charge of the preservation of parliamentary acts and documents, drafting of stenographic reports, bursars, technicians, etc.);
2. persons performing a public judicial function, such as, for example:
 - magistrates (ordinary magistracy of Courts, Appeal Courts, Supreme Court of Cassation, Superior Court of Waters, TAR, Council of State, Constitutional Court, Military Tribunals, popular judges of the Assize Courts, justices of the peace, honorary and aggregate deputy praetors, members of ritual arbitration panels and parliamentary commissions of enquiry, magistrates of the European Court of Justice, as well as of the various international courts, etc.);
 - persons carrying out related functions (judicial police officers and agents, financial police and carabinieri, chancellors, secretaries, judicial custodians, bailiffs, witnesses, conciliation messengers, bankruptcy receivers, operators in charge of issuing certificates at court registry offices, experts and consultants of the Public Prosecutor, liquidators in bankruptcy proceedings, liquidators in composition with creditors proceedings, extraordinary commissioners of the extraordinary administration of large enterprises in crisis, etc.);
3. persons performing a public administrative function, such as, for example:
 - employees of the State, of international and foreign bodies and of territorial bodies (officials and employees of the State, of the European Union, of supranational bodies, of foreign States and of territorial bodies, including Regions, Provinces, Municipalities and Mountain Communities; persons who perform ancillary functions with respect to the institutional purposes of the State, such as members of the municipal technical office, members of the building commission, head of the administrative office of the amnesty office, municipal messengers, persons in charge of practices concerning the occupation of public land, municipal correspondents in charge of the employment office, employees of State-owned companies and municipalised companies; persons in charge of tax collection, health personnel of public facilities, personnel of ministries, superintendencies, etc.);
 - employees of other public, national and international bodies (officials and employees of the Customs and Monopolies Agency, the Bank of Italy, the Supervisory Authorities, public welfare institutions, ISTAT, the UN, the FAO, etc.).

Activities that, although governed by rules of public law or authoritative acts, nevertheless consist in the performance of simple orderly tasks or the performance of purely material work are not considered public services.

The figures of the public official and the person in charge of a public service are identified not on the basis of the criterion of belonging to or being dependent on a public body, but with reference to the nature of the activity concretely carried out by that body, i.e. public function and public service respectively.

Even a person who is not a member of the Public Administration (hereinafter 'PA') may therefore be qualified as a public official or a person in charge of a public service, when he performs one of the activities defined as such in Articles 357 and 358 of the Criminal Code (e.g. employees of banking institutions who are entrusted with tasks falling within the 'public service').

Moving on to analyse the potential risk profile of the area of relations with public institutions and bodies, the management of relations with the PA exposes the Company to the risk of committing or participating in the offences of:

- concussione (art. 317 c.p.), corruzione per l'esercizio della funzione (art. 318 c.p.), corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.), corruzione in atti giudiziari (art. 319-ter c.p.), corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), istigazione alla corruzione (art. 322 c.p.), embezzlement, extortion, undue inducement to give or promise benefits, bribery and incitement to bribery of members of international courts or bodies of the European Communities or international parliamentary assemblies or international organisations and officials of the European Communities and foreign states (Article 322-bis of the criminal code);
- trafficking in unlawful influence (Article 346-bis of the Criminal Code);
- Undue inducement to give or promise benefits (Article 319-quater of the Criminal Code)
- inducement not to make statements or to make false statements to the judicial authorities (Article 377-bis of the criminal code).

Such offences could in abstract be committed, for instance, through the giving or promising of money or other benefits (including through a person exercising unlawful influence) to

- a PA official not to have measures/sanctions issued against the Company as part of audits or other regulatory requirements to which the Company is subject;
- an official of the PA to make certain non-compliant data admissible as public funding reports;
- an employee called to testify, in order to induce him/her to make false statements (or not to make statements) to the judicial authority;
- a witness at a trial, in order to induce him/her to make false statements (or not to make statements) to the judicial authority.

Moreover, the management of relations with the PA exposes the Company to the risk of committing or participating in the offences of:

- fraud (Article 640(2)(1) of the Criminal Code), aggravated fraud to obtain public funds (Article 640-bis of the Criminal Code), embezzlement of public funds (Article 316-bis of the Criminal Code) and misappropriation of public funds (Article 316-ter of the Criminal Code). As regards the purposes and methods of commission of the unlawful conduct, they are identified in the abstract as, for example:
 - in the alteration of the content of documentation - in terms of incompleteness, incorrectness, etc. - intended for public bodies responsible for personnel belonging to protected categories, or relating to requests for authorisations or for obtaining public funds;
 - transmitting documentation containing false information to the tax authorities in order to obtain a tax refund that is not due;
 - sending to social security bodies, local administrations or divisions thereof communications containing false data with a view to obtaining any advantage or benefit from the Company;
- obstructing the exercise of the functions of the public supervisory authorities (Article 2638 of the Civil Code), which takes the form, in abstract terms, of, for instance, preparing and sending to the supervisory authorities untrue documentation or concealing and/or omitting relevant documents and information during inspections;

- Computer fraud (Article 640-ter(1) of the Criminal Code). This offence occurs when, by altering the operation of a computer or telecommunications system or manipulating the data contained therein, an unfair profit is obtained causing damage to the State or another public body. Interference may take various forms, at the stage of:
 - data collection and input;
 - data processing;
 - emission of data.

In all these cases, the intervention takes place on the memory of a computer on the proper functioning of which the material author of the offence interferes in order to obtain undue enrichment to the detriment of the State or other public body. For example, as regards the ways in which the offence is committed, these could in abstract be:

- the modification of information relating to the accounting situation of an existing contractual relationship with a public body;
- the alteration of tax and/or social security data contained in a database belonging to the PA;
- bribery among private individuals (Article 2635(3) of the Civil Code) and incitement to bribery among private individuals (Article 2635-bis(1) of the Civil Code), where, for example, a Company representative bribes or attempts to bribe, even through an intermediary, by offering or promising money or other benefits, the opposing party's lawyer or technical consultant belonging to a professional firm.

3.12.2. ACTIVITIES AT RISK AND ENTITIES INVOLVED

The Company has a variety of relations with the PA in the performance of its activities (e.g. INAIL-INPS, Labour Inspectorate, ISTAT). Below are the corporate bodies involved in the management of the activity at risk relations with public institutions and bodies (Country Activity Leader - Functions involved Legal Business Partner, Sales Finance, Payroll Specialist and HR).

3.12.3. SPECIFIC CONTROL PROTOCOLS

Relations with Public Institutions and Bodies must be managed not only in accordance with the principles contained in the Code of Ethics and Conduct, but also in compliance with the Guidelines defined by the Company, which provide for

- the following general criteria that should inspire relations with the PA:
 - when managing the different relationships with the various PA bodies, an appropriate separation of functions must be ensured;
 - in the event of participation in tenders of any kind organised by the PA, it is necessary to comply with all the provisions of the law and regulations governing the tender, refraining from conduct that may, in any way, unduly disrupt or influence the conduct of the tender;
 - Contributions in cash or in products and services to charities, cultural and educational institutions, schools and foundations are permitted, provided they are made with the utmost transparency and in compliance with the rules, internal procedures and regulations in force;
 - with reference to the management of authorisations, licences and administrative concessions, corporate activities must be carried out in compliance with the limits of the concession, authorisation or licence obtained. Any critical issues or difficulties of any kind must be highlighted in writing and managed by the competent corporate functions in compliance with the law and other applicable regulations;
 - computer procedures must be used in the correct manner;
 - it is prohibited to:

Special Part

- submit untruthful declarations to national or Community public bodies in order to obtain public grants, contributions or subsidised financing;
- allocate sums received from national or Community public bodies by way of disbursements, contributions or financing for purposes other than those for which they were intended;
- making any form of contribution to political parties, public officials, etc. through, for example, direct or indirect payments, loans, advances, deposits or donations of money, products or services;
- checking all documents (e.g. declarations) to be sent to the PA and submitting them for signature by the authorised attorney;
- hierarchical escalation criteria in the management of relations with the PA, especially where critical issues are identified that cannot be resolved in the ordinary course of business;
- the prompt reporting to the competent corporate functions and to the Supervisory Board of any anomalous situation;
- Adequate traceability, archiving and preservation of documentation relating to the main dealings with the PA (e.g. through the exchange of e-mails, drafting/subscription of minutes, communication by e-mail to one's hierarchical superior of meetings held with PA representatives).

With regard to inspection/audit activities by PA representatives, Hitachi Vantara Italia personnel must comply with the criteria of:

- quality and timeliness of communications to supervisory authorities;
- reliability of communications;
- proper formalisation of activities;
- timely and complete provision of the required documentation and maximum availability and cooperation in the performance of inspections/verification activities.

Please also refer to the previous risk areas for a description of the specific control protocols in the management of further activities that may involve a relationship with a PA representative.

3.13. DONATIONS, GIFTS AND GRATUITIES

3.13.1. DESCRIPTION OF THE POTENTIAL RISK PROFILE

The management of donations, gifts and gratuities constitutes an instrumental mode through which, in principle, the offences of:

- corruzione per l'esercizio della funzione (art. 25 D.Lgs. 231/01 - art. 318 c.p.), corruzione per un atto contrario ai doveri d'ufficio (art. 25 D.Lgs. 231/01 - art. 319 c.p.), corruzione di persona incaricata di un pubblico servizio (art. 25 D.Lgs. 231/01 - art. 320 c.p.), istigazione alla corruzione (art. 25 D.Lgs. 231/01 - art. 322 c.p.), embezzlement, extortion, undue induction to give or promise benefits, bribery and incitement to bribery, abuse of office of members of international courts or bodies of the European Communities or international parliamentary assemblies or international organisations and officials of the European Communities and foreign States (Article 322-bis of the criminal code);
- trafficking in unlawful influence (Article 346-bis of the Criminal Code);
- inducement not to make statements or to make false statements to the judicial authorities (Article 25-decies of Legislative Decree 231/01 - Article 377-bis of the criminal code);
- Undue inducement to give or promise benefits (Article 25 of Legislative Decree 231/01 - Article 319-quater of the criminal code);
- bribery among private individuals and incitement to bribery among private individuals (Article 25-ter, Legislative Decree 231/01 - Articles 2635(3) and 2635-bis(1) of the Civil Code).

Such offences could, in fact, be committed in the abstract through:

- the granting or promising of gifts/hospitality/sponsorships to public or similar persons or to private persons, in order to obtain in exchange advantages, favourable treatment, non-application of a penalty, etc;
- the granting or promising of company goods/services free of charge to public or similar persons or to private parties, in order to obtain in exchange advantages, favourable treatment, non-application of a penalty, etc;
- Invitations to events, which are appreciated by public or similar persons or private persons in order to obtain in exchange advantages, favourable treatment, non-application of a sanction, etc.

Lastly, this area is abstractly at risk with regard to the offence of undue use and falsification of non-cash payment instruments (Article 493 ter of the Criminal Code) in the event that a senior person or subordinate of HVI makes payments for gifts or entertainment expenses by means of a payment card not in his name or another instrument other than cash, and, therefore, by means of undue use, in order to obtain an advantage for the Company from that transaction. The offence could be committed in the event that a senior person or subordinate of HVI makes a payment or even a withdrawal by means of a payment card not in his name or by means of an instrument other than cash, and, therefore, by means of misuse, in order to obtain an unlawful advantage for the Company from that transaction.

3.13.2. ACTIVITIES AT RISK AND ENTITIES INVOLVED

The entities involved in the management of risk activity Management of donations, gifts and gratuities (Country Leader) are highlighted below.

3.13.3. SPECIFIC CONTROL PROTOCOLS

The management of gifts/giveaways/hospitality etc. received/offered by the Company's personnel must be carried out in accordance with the principles contained in the Code of Ethics and Conduct and in compliance with the Guidelines defined by the Company, which provide:

- that expenses relating to hospitality and representation shall be reasonable and in any event such that they cannot be construed as aimed at obtaining favourable treatment from the Recipient;

- the express prohibition of facilitation payments for the purpose of favouring services in any way due from the PA or private third parties;
- formalised controls on the approval of gifts and entertainment expenses;
- Formal verification of the expenditure slips and correspondence between the expenditure slips and the sums entered in the accounts;
- gifts and entertainment expenses must:
 - be reasonable and in any case such that they cannot be interpreted as aimed at obtaining favourable treatment from the Recipient;
 - be directed towards Addressees who perform roles inherent to the company's activities and who meet the generally recognised requirements of reputation and honourableness;
 - take into account the profile of the Addressee, with regard to customs in professional relations and respect for local cultures;
 - be carried out by directors, managers and employees depending on the activity carried out and the role held within the Company;
 - be provided for by specific company provisions;
 - be in line with the budget and in any case authorised in advance by the competent manager of the Company, in accordance with the applicable company procedures.

In particular, for gifts and entertainment expenses, a monitoring report is prepared by the competent structures, containing information to trace who has offered or received the gift, the date of the offer or receipt of the gift, the current or estimated value, an indication of any acceptance or refusal and the reasons thereof.

In any case, any form of gift to representatives of other private companies, or to their family members, that may induce them to secure any advantage for the Company is forbidden. Gifts offered or received - except those of a modest amount - must be adequately documented.

As regards the management of gifts/giveaways/hospitality expenses etc. received/offered by Company personnel, Group Policy defines the limits and criteria on the basis of which the Company admits such transactions. In particular, provision is made with reference to the offer/receipt of gifts and gratuities or the incurring of hospitality expenses (meals/entertainment):

- the prohibition to offer/receive gifts exceeding the value of \$30, and to offer/receive hospitality expenses exceeding the value of \$100, without the prior written approval of the Local Legal Counsel or the Compliance Department;
- gifts must consist of gadgets containing the Company's logo and may not consist of money or its equivalent;
- a ban on offering/receiving gifts to spouses or family members of PA representatives;
- that no gifts/giveaways are to be offered/received in violation of applicable laws.