



ZTE ITALIA S.R.L.

Organisation, Management and Control Model
pursuant to Italian Legislative Decree no. 231 of 8 June 2001

Approved by the Board of Directors of 21th March 2018

TABLE OF CONTENTS

TABLE OF CONTENTS.....	2
DEFINITIONS.....	5
STRUCTURE OF THIS DOCUMENT.....	8
GENERAL SECTION.....	9
1. Italian Legislative Decree no. 231 of 8 June 2001.....	9
1.1. Liability of entities for offences.....	9
1.2. Categories of so-called predicate offences.....	9
1.3. Criteria for imputation of liability to the entity; exemption from liability.....	12
1.4. Indications of the Decree regarding the characteristics of the organisation, management and control model.....	14
1.5. Penalties.....	15
2. ZTE Italia: The Company and its <i>corporate governance</i> and internal control system.....	18
2.1. The Company and the Group.....	18
2.2. Corporate governance system.....	18
2.3. Internal control system.....	19
3. Methodology for preparing the Model; changes and updating of the Model.....	22
4. Persons covered by the Model and rules governing relations with third parties.....	24
5. Supervisory Body.....	25
5.1. Function.....	25
5.2. Requirements and composition of the Supervisory Body.....	25
5.3. Eligibility requirements for members of the Supervisory Body.....	27
5.4. Appointment, revocation, replacement, forfeiture and withdrawal.....	28
5.5. Activities and powers.....	29
5.6. Information flows to the SB and whistleblowing schemes.....	31
6. Disciplinary system.....	35
6.1. General principles.....	35
6.2. Violations of the Model.....	36
6.3. Measures against employees.....	37
6.4. Violations of the Model by executives and related measures.....	40
6.5. Measures against members of the Executive Body and the Sole Auditor.....	42
6.6. Measures against members of the SB and third parties.....	44
7. Communication of the Model and training of recipients.....	44
SPECIAL SECTION.....	46
8. Introduction.....	46
9. Predicate offences relevant to the Company.....	46
10. General controls.....	47
11. Offences against public administration.....	49

11.1.	Applicable offences	49
11.2.	At-risk activities	53
11.3.	Controls	54
12.	IT-related felonies and unlawful processing of data	67
12.1.	Applicable offences	67
12.2.	At-risk activities	69
12.3.	Controls	70
13.	Felonies committed by criminal organisations and transnational offences	71
13.1.	Applicable offences	71
13.2.	At-risk activities	73
13.3.	Controls	73
14.	Offences against industry and trade	76
14.1.	Applicable offences	76
14.2.	At-risk activities	76
14.3.	Controls	77
15.	Corporate offences, including those of corruption between private persons	81
15.1.	Applicable offences	81
15.2.	At-risk activities	84
15.3.	Controls	85
16.	Felonies against individual's freedoms	88
16.1.	Applicable offences	88
16.2.	At-risk activities	89
16.3.	Controls	89
17.	Manslaughter and serious or very serious injuries committed in violation of occupational health and safety protection regulations	92
17.1.	Applicable offences	92
17.2.	At-Risk Activities; the provisions of article 30 of Legislative Decree no. 81 of 9 April 2008	93
17.3.	Controls	94
18.	Receiving, laundering and using money, goods or benefits of unlawful provenance, including self-laundering	99
18.1.	Applicable offences	99
18.2.	At-risk activities	100
18.3.	Controls	101
19.	Offenses relating to the infringement of copyright	103
19.1.	Applicable offences	103
19.2.	At-risk activities	103
19.3.	Controls	104
20.	Inducement to make no declarations or to make mendacious declarations to the judiciary authority	104
20.1.	Applicable offences	104
20.2.	At-risk activities; controls	105



- 21. Environmental offences..... 106
 - 21.1. Applicable offences 106
 - 21.2. At-risk activities 107
 - 21.3. Controls 107
- 22. Use of foreign citizens illegally present in the country 109
 - 22.1. Applicable offences 109
 - 22.2. At-risk activities 109
 - 22.3. Controls 110

DEFINITIONS

At-risk activities	activities of the Company in which there is a risk of committing crimes as per the Decree or relevant to the management of financial resources
CCNL	National Collective Labour Contract
Code of Conduct	Code of conduct of the Group adopted by the Company and documents supplementing it
Employees	persons having an employment or self-employment contract with the Company, as well as temporary and seconded workers at the Company
Legislative Decree No. 231/2001 or Decree	Italian Legislative Decree no. 231 of 8 June 2001
Confindustria Guidelines	Confindustria document (approved on 7 March 2002 and updated at March 2014) for the preparation of the Organisation, Management and Control models as per Legislative Decree No. 231/2001.
Model	Model for organisation, management and control pursuant to Legislative Decree No. 231/2001
Supervisory Body or SB	Body provided for by article 6 of Legislative Decree No. 231/2001, which is entrusted with

PA

the task of supervising the operation and observance of the Model and its updating

Public Administration, which means jointly:

- Public Entities: entities created through an act of the State to meet the organizational or functional needs of the State, such as municipalities and provinces, land reclamation or irrigation consortia, chambers of commerce, the Civil Aviation Authority (ENAC), INPS, INAIL, and IPSEMA;

- Public Officials: subjects who carry out a legislative, judicial or administrative public function and who can form or express the will of the Public Administration through the exercise of authoritative or certifying powers, such as, for example, members of state and territorial administrations, supranational administrations (e.g., of the European Union), the Police and Guardia di Finanza (Italian Tax Police), Chambers of Commerce, the Housing Commissions, judges, bailiffs, judicial officers, the subsidiary bodies of the justice administration (e.g., Official Receivers), administrators and employees of public bodies, private individuals vested with powers to form or express the will of the Public Administration;

- persons subjects in charge of a public service: persons who, for whatever reason, provide a public service, to be understood as an activity regulated in the same forms as a public function, but characterised by the lack of powers typical of that function, with the exclusion of the performance of simple public order tasks and of the provision of purely material work. A private individual or employee of a private company may also be qualified as a person in charge of a public service when carrying out activities aimed at the pursuit of a public purpose and the protection of a public interest.

Procedures

procedures, policies, organisational provisions, service orders and all other provisions, measures and acts of the Company that implement the control principles contained in this document, including the Quality Manual conforming to the standard UNI EN ISO 9001 that the Company is provided with

ZTE Italia or Company

ZTE Italia S.r.l.

STRUCTURE OF THIS DOCUMENT

This document is composed of a General and a Special Section.

The General Section discusses the following issues:

- regulations as per Legislative Decree No. 231/2001;
- the Company's governance system;
- method of preparing the Model;
- persons to whom the provisions of the Model apply;
- the composition and functioning of the Supervisory Body;
- the system of sanctions to monitor violations of the Model;
- dissemination of the Model and staff training.

The Special Section, on the other hand, contains the rules governing at-risk activities and sets out the controls, aimed at or in any case suitable for reducing the risk of committing the crimes set out by the Decree. These controls are contained and implemented in the Procedures.

The following is also an integral part of the Model:

- the document "Control & risk self assessment and Gap analysis pursuant to Legislative Decree No. 231/2001," which formalises the results of the Control and Risk Self Assessment activity aimed at identifying at-risk activities;
- the Code of Conduct, which defines the principles and rules of conduct of the Company;
- Procedures.

These acts and documents are available in accordance with the procedures established for their dissemination to Company personnel.

GENERAL SECTION

1. Italian Legislative Decree no. 231 of 8 June 2001

1.1. Liability of entities for offences

Legislative Decree No. 231 of 8 June 2001 introduces and regulates the administrative liability deriving from offences of collective entities. This form of liability combines aspects of the criminal and administrative penalty system. According to the Decree, an entity is punished with a penalty of an administrative nature, as it is responsible for an administrative offence, but the penalty system is based on the criminal trial: the competent authority that prosecutes the offence is the Public Prosecutor and a criminal court hands down the penalty. The criminal liability of entities is therefore formally administrative in nature, but is essentially a criminal liability.

Moreover, it is separate and independent from that of the natural person who commits the offence, so much so that it subsists even if the perpetrator has not been identified, or when the offence has been extinguished for a reason other than amnesty. In any case, the entity's liability is added to, and does not substitute, that of the natural person who committed the offence.

The scope of application of the Decree is very broad and covers all entities having legal personality (including, of course, companies), associations, including without legal personality, and public economic bodies. The legislation in question is not applicable to the State, to regional and local authorities, non-economic public bodies and bodies with constitutional functions (such as political parties and trade unions).

1.2. Categories of so-called predicate offences

An entity can be held liable only for the offences - so-called predicate offences - indicated as a source of liability by the Decree or, in any case, by a law to have taken effect before the act constituting an offence was committed.

At the date of approval of this document, predicate offences belong to the categories indicated below:

- Offences against Public Administration (Articles 24 & 25);
- IT-related felonies and unlawful processing of data (article 24-bis);
- Felonies committed by criminal organisations (Article 24-ter);
- Forgery of money, money values having legal tender or revenue stamps and instruments or identification signs (Article 25-bis)
- Felonies against industry and commerce (article 25-bis.1);
- Corporate offences, including those of corruption between private persons (Article 25-ter)
- Felonies committed for purposes of terrorism or designed to subvert democracy (Article 25-quater);
- Mutilation of women's genitals (Article 25-quater.1)
- Felonies against individual's freedoms (Article 25-quinquies);
- Market abuse (Article 25-sexies);
- Manslaughter or serious bodily harm committed with breach of laws governing the safeguarding of workplace health and safety (Article 25-septies);
- Handling stolen goods, laundering and use of money, assets or benefits whose origin is illegal (Article 25-octies)
- Felonies regarding breach of copyright (Articles 25-novies);
- Inducements not to make statements or to make false statements to the courts (Article 25-decies);
- Environmental crimes (Article 25-undecies);
- Use of illegally staying third country nationals (Article 25-duodecies);

- Transnational crimes (Article 10 of Italian Law No. 146 of 16 March 2006)¹;

¹ The modifications to the types of offences provided for by the Decree were made by the following legislative acts: Decree Law No. 350 of 25 September 2001, which introduced article 25-bis "Forgery of currency, public credit cards, duty stamps," subsequently expanded and amended into "Forgery of money, money values having legal tender or revenue stamps and instruments or identification signs" by Law no. 99 of 23 July 2009; Legislative Decree no. 61 of 11 April 2002, which introduced the article 25-ter "Corporate Offences"; Law no. 7 of January 14, 2003, which introduced article 25-quater "Felonies committed for purposes of terrorism or designed to subvert democracy"; Law no. 228 of 11 August 2003, which introduced article 25-quinquies "Felonies against individual's freedoms"; Law no. 62 of 18 April 2005, which introduced article 25-sexies "Market abuse"; Law no. 7 of 9 January 2006, which introduced article 25-quater.1 "Mutilation of women's genitals"; Law no. 146 of 16 March 2006, which provides for the liability of entities for transnational crimes; Law no. 123 of 3 August 2007, which introduced the article. 25-septies "Manslaughter and serious or very serious negligent injuries, committed in violation of accident prevention and occupational health and safety protection regulations," subsequently amended to "Manslaughter or serious or very serious injuries, committed in violation of the regulations on health and safety protection at work" by Legislative Decree No. 81 of 9 April 2008; Legislative Decree no. 231 of 21 November 2007, which introduced art. 25-octies "Receiving stolen goods, money laundering and use of money, goods or utilities of illegal origin," subsequently amended to "Receiving stolen goods, money laundering and use of money, goods or utilities of illegal origin, as well as self laundering" by Law no. 186 of 15 December 2014; Law no. 48 of 18 March 2008, which introduced the article 24-bis "IT-related crimes and unlawful processing of data"; Law no. 94 of 15 July 2009, which introduced article 24-ter "Felonies committed by criminal organisations"; Law no. 99 of 23 July 2009 - already mentioned - which introduced article 25-bis. 1 "Felonies against industry and commerce" and Article 25-novies "Felonies regarding breach of copyright"; Law No. 116 of 3 August 2009, which introduced article 25-novies (later renumbered article 25-decies by Legislative Decree No. 121 of 7 July 2011) "Inducement not to make statements or to make false statements to Judicial Authority"; Legislative Decree No. 121/2011 - already mentioned - which introduced article 25-undecies "Environmental crimes"; Legislative Decree No. 109 of 16 July 2012, which introduced article 25-duodecies "Employment of illegally staying third-country nationals"; Law no. 190 of 6 November 2012, which amended articles 25 and 25-ter; Law no. 68 of 22 May 2015, which amended article 25-undecies; Law no. 69 of 30 May 2015, which amended article. 25-ter; Law no. 199 of 29 October 2016, which amended Article 25-quinquies; Legislative Decree No. 38 of 15 March 2017, which amended Article 25-ter; Law no. 161 of 17 October 2017, which integrated art. 25-duodecies with the insertion of the reference to paragraphs 3, 3-bis, 3-ter and 5 of art. 12 of Legislative Decree no. 286/1998, concerning the conduct of those who "*direct, organize, finance, transport foreigners to the territory of the State or carry out other acts aimed at illegally obtaining their entry into the*

- Racism and Xenophobia offences (Article 25-terdecies).

The entity may also be called upon to answer before Italian courts for alleged offences committed abroad under the following conditions:

- The general conditions of admissibility laid down in Articles 7, 8, 9 and 10 of the Criminal Code exist in order to be able to prosecute an offence committed abroad in Italy;
- the entity has its head office in the territory of the Italian State;
- the State where the offence was committed does not prosecute the entity.

1.3. **Criteria for imputation of liability to the entity; exemption from liability**

In addition to committing one of the predicate offences, in order for the entity to be punished pursuant to Legislative Decree no. 231/2001, other regulatory requirements should be integrated. These additional criteria of corporate liability can be distinguished into “objective” and “subjective.”

The first objective criterion is supplemented by the fact that the offence was committed by a person linked to the entity by a qualified relationship. In this respect, a distinction is made between:

- “persons in a top management position”: i.e., persons holding positions of representation, administration or management of the entity, such as, directors, general managers or directors of an autonomous organisational unit and, in general, persons who manage, also de facto, the entity itself or one of its autonomous organisational units;
- “subordinate subjects”: i.e., all those who are subject to the management and supervision of persons in top management positions. This category includes employees and those persons who, though they are not part of personnel, have a task to perform under the direction and control of top management.

territory of the State” or promote their permanence “in order to obtain an unfair profit from the condition of illegality”; Law no. 167 of November 20, 2017, which included in the Decree art. 25-terdecies entitled “racism and xenophobia”.

The identification of the persons referred to above is independent from the contractual classification of the relationship that they have with the entity; in fact, they must also include persons not belonging to the personnel of the entity, if they act in the name, on behalf or in the interest of the entity itself.

Another objective criterion is represented by the fact that the offence must be committed in the interest or to the advantage of the entity; it is sufficient that at least one of the two alternative conditions is present (in this sense, see Penal Cass. no. 3615, 20 December 2005):

- interest subsists when the perpetrator of the offence acted with the intent to favour the entity, regardless of whether this objective was actually achieved;
- advantage subsists when the entity has drawn - or could have drawn a positive, economic or other result from the offence.

As regards the subjective criteria for imputation of liability to the entity, these relate to the preventive tools that it has adopted in order to prevent the commission of one of the predicate offences in the exercise of business.

In the event of an offence committed by a person in a top management position, the Decree provides for an exemption from liability for the entity if it proves that:

- management adopted and effectively implemented, before the fact, suitable organisational, management and control models for preventing offences of the kind committed;
- the task of supervising the operation and observance of models, and the updating of models was delegated to a specific body of the entity with autonomous powers of initiative and control;
- the person in a senior position committed the offence by fraudulently circumventing the models;
- there has been no omission or insufficient supervision by that body.

In the case of offences committed by subordinate persons, the entity may instead be held liable only if it is ascertained that the commission of the offence was made possible by failure to comply with management or supervisory obligations, however excluded if, before the commission of the crime, the entity adopted organisational, management and control models suitable for preventing offences of the type committed.

1.4. Indications of the Decree regarding the characteristics of the organisation, management and control model

The Decree simply regulates some general principles regarding the organisation, management and control model, providing for the following minimum content:

- identification of the activities in relation to which offences may be committed;
- provision for specific protocols aimed at planning training and the implementation of the decisions of the entity in relation to the offenses to prevent;
- identification of procedures for managing financial resources which are fit to prevent the commission of offences;
- adoption of introduce a disciplinary system to punish noncompliance with the measures set out in the model;
- identification of information flows to the Supervisory Body;
- Regarding the type and size of the organisation and the type of activity performed, the model provides for measures to ensure performance of the activity in compliance with the law and to discover and promptly eliminate risk situations.

Pursuant to the Law no. 179/2017 (*“Provisions for the protection of whistleblowers who report offences or irregularities which have come to their attention in the context of a public or private employment relationship”*), in order to be compliant with the whistleblowing regulations, a model shall now provide for:

- more than one channels that, while ensuring the confidentiality of the identity of the whistleblower, allow the employees to submit detailed reports of illegal conduct or violations of the 231 Model (one of these channels has to be implemented via informatics tool);
- the prohibition of discriminatory action against the whistleblower (*i.e.* anti-retaliation measures);
- adequate sanctions for those who violate the above-mentioned anti-retaliation measures and for those who – intentionally or negligently – file reports that prove to be unfounded.

The Decree establishes that the model is subject to periodic verification and updating, both in the event that significant violations of the regulations are detected and in the event of significant changes in the organisation or activity of the entity.

1.5. Penalties

The penalty system provided for by Legislative Decree No. 231/2001 is divided into four types of sanctions, to which the body may be subjected in the event of conviction pursuant to the Decree:

- fine: it is always applied where the court considers the entity to be responsible and shall be calculated by means of a quota-based system, which shall be determined by the court in number and amount; the number of quotas, to be applied between a minimum and a maximum that vary according to the type of offence, depends on the seriousness of the offence, on the degree of responsibility of the entity, on the activity carried out to eliminate or mitigate the consequences of the crime or to prevent the commission of other offences; the amount of the single quota must be established, instead, between a minimum of €258.00 and a maximum of €1,549.00, depending on the economic and capital conditions of the entity;
- disqualification measures: disqualification measures are applied in addition to fines, but only if they are expressly provided for the offense being prosecuted and that at least one of the following conditions subsists:

- the entity has gained significantly from the offense and the offense was committed by a senior manager, or by a subordinate, but only when the commission of the offense has been facilitated by serious deficiencies in the organisation;
- in case of reiterated offences.

Disqualification measures provided for by the Decree are:

- disqualification from exercising the activity;
- suspension or cancellation of authorisations, licences or concessions serving to commit the unlawful act;
- prohibition on entering into contracts with PA, unless done so in order to obtain a public service;
- exclusion from benefits, loans, contributions or subsidies and possible cancellation of those already granted;
- prohibition on publicising goods or services.

Exceptionally applicable with permanent effects, disqualification measures are temporary, with a duration ranging from three months to two years and relate specifically to the specific activity of the entity to which the offence refers. They can also be applied as a precautionary measure, where there are serious indications of the liability of the entity and there are reasonable and specific elements indicating a real danger that offenses of the same nature as the one being prosecuted can be committed;

- Confiscation: conviction always involves the order to confiscate the price or profit of the offence or property or other assets of equivalent value;
- Publication of the conviction: it can be ordered when the entity is sentenced to disqualification and consists in publication at the expense of the entity of the sentence, in abridged form or in full, in one or more newspapers indicated by the judge in the judgement as well as by means of posting in the municipality where the entity has its head office.



Administrative penalties imposed on the entity are time-barred five years after the date of commission of the offence constituting the administrative offence.

The final conviction of the entity is entered in the national register of administrative penalties for offences.

The Decree also regulates the entity's liability in case of transformation, merger, demerger and transfer of the company.

In case of transformation of the entity, liability for offences committed prior to the date on which the transformation took effect remains unaffected. The new entity will be the recipient of the penalties applicable to the original entity for acts committed prior to the transformation.

In the event of a merger, the entity resulting from the merger, also by incorporation, is liable for the offences for which the entities involved in the merger were liable.

In the case of demerger, the demerged entity retains liability for offences committed prior to the date on which the demerger took effect and the entities benefiting from the demerger are jointly and severally obliged to pay the fines imposed on the demerged entity within the limits of the value of the net assets transferred to each individual entity, except in the case of entities to which the business unit in which the offence was committed has also been partially transferred; disqualification applies to the entity (or entities) retaining or receiving the business unit within which the offence was committed.

In the event of assignment or contribution of an undertaking in relation to which an offence has been committed, the assignee is jointly and severally liable for payment of the fine, without prejudice to the right to make first claims for payment on the part of the assigning body and subject to the limit of the value of the undertaking and to the limit of the fines recorded in the mandatory accounts, or otherwise of fines payable for unlawful acts about which the assignee was however aware.

2. ZTE Italia: The Company and its *corporate governance* and internal control system

2.1. The Company and the Group

ZTE Italia is part of a Group headed by ZTE Corporation, a global provider of telecommunications products and services, with over one hundred subsidiaries worldwide.

The Company, operating throughout Italy through the offices in Rome and Milan and a branch in Turin, carries out, with regard to public and private customers, activities for the purchase, sale, import and export, and distribution of software, hardware, machinery and equipment for telecommunications, as well as consulting, training and maintenance related to these products.

2.2. Corporate governance system

The Company's corporate governance system is currently structured as follows:

- Board of Directors: it is vested with the widest powers for the achievement of the Company's corporate purposes and for the ordinary and extraordinary management of the Company, except only for those acts which, in accordance with the law and the Articles of Association, fall under the exclusive remit of the Shareholders' Meeting;
- Sole Auditor: company management is controlled by a sole Auditor who also performs the role of independent auditor.

The Company's corporate governance system includes the Model and Procedures, aimed not only at preventing the offences set out by the Decree, but also at making the control system as efficient as possible.

The essential foundation of the Model is the Code of Conduct adopted by the Company, which formalises the ethical principles and values that inspire it in the conduct of its activities.

The Code recognizes the legal relevance and mandatory effectiveness of the ethical principles and behavioural standards described therein, also with a view to the prevention of corporate offences, and is based on its compliance with current legislation.

2.3. Internal control system

The internal control system of ZTE Italia, with particular reference to sensitive activities and consistent with the provisions of Confindustria Guidelines, is based on the following principles:

- clear identification of roles, tasks and responsibilities of the persons involved in the implementation of company activities (inside or outside the organisation);
- separation of tasks between who carries out an activity operationally, who controls it, who authorises it and who records it (where applicable);
- verifiability and documentability of ex-post transactions: the relevant activities carried out (especially in at-risk activities) are suitably formalised, with particular reference to the documentation prepared during their implementation. The documentation produced and/or available in paper or electronic form is filed by the Functions/persons involved;
- identification of preventive controls and ex-post, manual and automatic checks: manual and/or automatic controls are provided to prevent the commission of offences or to detect ex-post irregularities that could contrast with the Model's objectives. These controls are more frequent, articulated and sophisticated within those At-Risk Activities characterised by a higher risk profile of committing offences.

The components of the internal control system relate to the following elements:

- a system of ethical principles aimed at preventing the offences set out by the Decree;
- organisational system sufficiently formalised and clear;
- system of authorization and signature powers consistent with the assigned organizational and management responsibilities;
- management control system capable of providing timely notification of the existence and occurrence of critical situations;
- personnel communication and training system regarding the elements of the Model;
- adequate disciplinary system to sanction the violation of the Model's rules;

- system of operating procedures, whether manual or IT, aimed at regulating activities in the company's risk areas with appropriate controls;
- IT system for the performance of operational or control activities in the context of at-risk activities, or to support them.

With reference to the system of ethical principles, the communication and training system and the disciplinary system, reference should be made to the Code of Conduct and to paragraphs 6 and 7 of this General Section.

The Company's organisational system is set out through the preparation of a corporate organisational chart and the issuing of delegated functions and organisational provisions (service, job description, internal organisational directives), which provide a clear definition of the functions and responsibilities assigned to each local organisational unit.

The authorisation and decision-making system translates into an articulated and coherent system of delegation of functions and powers of attorney of the Company, based on the following principles:

- Proxies set out each management power with its responsibility and an appropriate position in the organisation chart, and are updated as a result of organisational changes;
- each proxy sets out and describes the management powers of the delegate and the person to whom the delegate reports hierarchically/functionally in a specific and unambiguous way;
- the management powers assigned with proxies and their implementation are consistent with company objectives;
- the delegate must have expenditure powers appropriate to the functions assigned to him/her;
- proxies are granted solely to persons with internal functional powers or specific tasks and provide for the extension of powers of representation and, possibly, expenditure limits.

The management control system adopted by ZTE Italia is divided into the various stages of annual budgeting, periodical report analysis and forecasting.

The system ensures:

- multiple parties involved, in terms of appropriate separation of functions for the processing and transmission of information;
- ability to provide timely notification of the existence and occurrence of critical situations through an adequate and timely system of information flows and reporting.

Article 6, paragraph 2, letter c) of the Decree expressly states that the Model must “*identify procedures for managing financial resources which are fit to prevent the commission of offences.*”

To this end, the management of financial resources is set out on the basis of principles based on a reasonable separation of functions, such as to ensure that all disbursements are requested, made and controlled by independent functions or entities as distinct as possible, to which, moreover, no other responsibilities are assigned such as to determine potential conflicts of interest.

Article 6, paragraph 2, letter b) of the Decree expressly states that the Model must “*provide for specific direct protocols and schedule training and implementation of decisions by the body regarding offences to be prevented.*”

To this end, the Company has adopted Procedures that allow it to regulate at-risk activities and therefore to guide and ensure the adoption and implementation of the control provided for by the Model. In particular, the Procedures ensure that the following principles are applied:

- clear formalisation of roles, responsibilities, methods and timing of implementation of the operational and control activities regulated;
- representation and regulation of the separation of tasks between the person who takes a decision (decision-making impulse), the person who authorises its implementation, the person who carries out the activities and the subject to whom control is entrusted;
- traceability and formalisation of each relevant activity of the process subject to the procedure in order to verify a posteriori the results achieved and evidence of the principles and control activities applied;
- adequate level of archiving of relevant documentation.

In order to safeguard the company's documentary and IT assets, adequate security measures are also provided to protect against the risk of loss and/or alteration of documentation relating to at-risk activities or unwanted access to data/documents.

In order to monitor the integrity of data and the effectiveness of the information systems and/or IT applications used to carry out operational or control activities in the context of at-risk activities, or to support them, the presence and operations of the following are guaranteed:

- user profiling systems in relation to access to modules or environments;
- rules for the correct use of company IT systems and aids (hardware and software support);
- automated mechanisms to control to systems;
- automated mechanisms for blocking or inhibiting access;
- automated mechanisms for the management of authorization workflows.

3. Methodology for preparing the Model; changes and updating of the Model

In order to prepare this document, in line with the provisions of the Decree, with the Confindustria Guidelines and with the indications inferable from jurisprudence, the Company has carried out a preventive activity of so-called Control and Risk self assessment.

The Control and Risk Self Assessment activities were conducted and coordinated by a Project Team made up of external consultants and directly involved the Company's Management.

In particular, these activities were divided into the following phases:

- acquisition and analysis of documents relevant to corporate governance and the company/group internal control system (e.g., organisational charts, codes of conduct, structures for delegation of powers and power of attorney, internal procedures, reports and minutes);

- preliminary identification of the at-risk activities for the various organisational units involved, with particular reference to those most affected by Legislative Decree no. 231/2001, also considering the identification of potential new risks of offence;
- identification of key officers to be involved in the interviews;
- conduct of finalised interviews:
 - identification/confirmation of at-risk activities, the operating procedures for their management and those involved;
 - identification of the potential (inherent) risks of committing the predicate offences attributable to individual at-risk activities;
 - analysis and evaluation of the controls/systems in place to mitigate the risks mentioned above and identification of possible areas for improvement;
- sharing with the Management of the findings and formalisation of these in a summary report (“Control & risk self assessment and Gap analysis pursuant to Legislative Decree 231/2001”), which is an integral part of this document.

This activity has led to the identification of adequate controls to be implemented in the control system in order to make it suitable for reducing the risk of commission of offences, as well as the effective implementation of the above controls in the control system by the individual key officers involved from time to time.

The Company has adopted the present version of its Organisation, Management and Control Model by resolution of the Board of Directors.

The Model must always be promptly modified or supplemented, exclusively by resolution of the Board of Directors, in the event that:

- there have been significant changes in the relevant legislation (e.g., introduction of new predicate offences in the Decree), as well as in the organisation or activity of the Company;

- violations or circumvention of the provisions contained therein have been found, which have demonstrated that they are not effective for the purpose of preventing offences.

Amendments to the Procedures are made by the Managers of the Functions concerned.

4. Persons covered by the Model and rules governing relations with third parties

The Model applies to:

- Directors and the Company's sole Auditor;
- employees of the Company;
- those who, in any case, work on a mandate and/or on behalf of the Company (e.g., by contract, such as consultants, or specific powers of attorney, such as counsel in court); these persons are under an obligation to respect the Model by means of specific contractual clauses.

In addition, any contract entered into by the Company with suppliers of goods or services must include a commitment on the part of the supplier or, if the supplier is a legal entity, a guarantee that its directors and employees will commit themselves to:

- comply with applicable legislation and not commit offences;
- comply with the principles of the Code of Conduct and of the Model (which will be brought to the attention of the supplier in the manner deemed most appropriate by the Company, e.g., through publication on its website or through specific communication);
- comply with any requests for information from the SB of the Company,

as well as to grant the Company the right to proceed with the application of forms of protection (e.g., termination of the contract, application of penalties, etc.), where there is a breach of these commitments and guarantees.

5. Supervisory Body

5.1. Function

In compliance with the Decree, the Company tasks its Supervisory Body with constantly supervising:

- compliance with the Model by the persons to whom the Model is applied, as identified in the previous paragraph, and the implementation of the Model's provisions in carrying out the Company's activities;
- the effectiveness of the Model in preventing the commission of the offences referred to in the Decree;
- the updating the Model.

5.2. Requirements and composition of the Supervisory Body

Jurisprudence and best practices concerning Legislative Decree no. 231/2001 have identified the following requirements of the Supervisory Body as indispensable:

- **Autonomy and independence:** the concepts of autonomy and independence do not have a valid definition in the absolute terms, but must be interpreted and set in the context of the operative complex in which they are to be applied. Since the Supervisory Body is tasked with verifying compliance, in the company's operations, with the controls applied; the position of the Supervisory Body within the body must ensure its independence from any form of interference and conditioning by any member of the body and, in particular, by top management, especially considering that the function exercised is also expressed in the oversight of the activities of persons in top management positions. Therefore, the Supervisory Body reports only to the Board of Directors when carrying out its functions.

Furthermore, in order to better guarantee the independence of the Supervisory Body, the Board of Directors provides it with resources, in number and skills proportionate to the assigned tasks, and approves, as part of the company budget process, an adequate allocation

of financial resources, proposed by the SB, which the latter may have at its disposal for any need for the proper performance of its tasks (e.g., specialist advice, travel, etc.).

The autonomy and independence of the individual members of the Supervisory Body must be determined on the basis of the function performed and the tasks assigned to them, identifying from whom and what it must be autonomous and independent in order to carry out these tasks. Consequently, each member must not hold decision-making, operational and management roles that may compromise the autonomy and independence of the entire SB. In any case, the requirements of autonomy and independence presuppose that members are not in a position, even potential, of personal conflict of interest with the Company.

In addition, members of the Supervisory Body must not:

- hold operational positions in the Company;
 - be a spouse, relative or similar within the fourth degree of directors of the Company;
 - be in any other situation of actual or potential conflict of interest;
- professional competence: the Supervisory Body must have technical and professional skills appropriate to the functions it is called upon to perform. Therefore, it is necessary that the Supervisory Body should include persons with adequate professional skills in economic, legal and analysis, risk control and management matters. In particular, the Supervisory Body must have the specialist technical skills necessary to carry out control and consultancy activities.

In order to ensure the professional skills that are useful or necessary for the activity of the Supervisory Body and to guarantee the professionalism of the Body (as well as, as already mentioned, its autonomy), the Supervisory Body is given a specific spending budget aimed at acquiring additional competences to its own, when necessary, outside the body. The Supervisory Body can thus, including with the help of external professionals, provide itself with competent resources expert, for example, in legal matters, company organisation, accounting, internal controls, finance and safety in the workplace, etc.;

- continuity of action: the Supervisory Body continuously carries out its activities.

Continuity of action should not be understood as “incessant operation,” since such an interpretation would necessarily impose a Supervisory Body exclusively within the entity, when this circumstance would instead lead to a decrease in the indispensable autonomy that must characterise the SB. Continuity of action means that the SB’s activity must not be limited to regular meetings of its members, but must be organised on the basis of an activity plan and the constant conduct of monitoring and analysis of the entity’s system of preventive controls.

In compliance with the above-mentioned principles, and taking into account the structure and operations of ZTE Italia, the Supervisory Body of the Company is composed, in collegial form, of two members, not members of the Company’s personnel.

5.3. Eligibility requirements for members of the Supervisory Body

The role of member of the Supervisory Body cannot be entrusted to a person who is:

- suspected or convicted, including with a sentence not yet final or suspended, except for the effects of rehabilitation:
 - for one or more of the offences provided for by Legislative Decree no. 231/2001;
 - for any offence with criminal intent;
- prohibited, disqualified, foreclosed or convicted, including with a sentence that is not yet final, to a penalty that results in disqualification, even temporary, from public offices or inability to hold a management position;
- submitted or has been subjected to preventive measures pursuant to Legislative Decree no. 159 of 6 September 2011 (“Code of anti-mafia laws and preventive measures, as well as new provisions on anti-mafia documentation, pursuant to articles 1 and 2 of Law no. 136 of 13 August 2010”);

- subject to the ancillary administrative penalties referred to in article 187-quater of Legislative Decree no. 58 of 24 February 1998.

5.4. Appointment, revocation, replacement, forfeiture and withdrawal

The Board of Directors appoints the Supervisory Body, justifying the decision concerning the choice of each member, after having verified that the requirements set forth in the preceding paragraphs are met, basing this decision on the curricula as well as on the official and specific statements directly collected from the candidates. In addition, the Board of Directors shall receive a declaration attesting to the absence of the reasons for ineligibility referred to in the previous paragraph from each candidate.

After formal acceptance of the nominees, the appointment is communicated at all company levels, through internal communication.

The Supervisory Body has its own Rules of Procedure, approving their contents and submitting them to the Board of Directors.

The SB holds office for three years. The members of the SB may be re-elected at the end of their term of office.

Withdrawal from office as a member of the SB can only take place through a resolution of the Board of Directors for one of the following reasons:

- the loss of the requirements set out in the previous paragraphs;
- non-performance of the obligations relating to the task entrusted;
- lack of good faith and diligence in the exercise of their duties;
- non-cooperation with other members of the SB;
- unjustified absence from more than two meetings of the SB
- breaches of confidentiality obligations or retaliatory or discriminatory acts against those who have reported illegal conduct or a violation of the Model, for reasons directly or indirectly

related to the report (including the violation of the anti-retaliatory provisions provided for the whistleblowing legislation);

- performing with malicious intent or gross negligence of reports that prove to be unfounded.

Each member of the SB is under an obligation to inform the Board of Directors, through the Chairman of the SB, of the loss of the requirements referred to in the paragraphs above.

The Board of Directors revokes the appointment of the member of the SB who is no longer eligible and, after adequate motivation, immediately replaces him/her.

Before the expiry of the term of office, any incapacity or impossibility to carry out the task shall constitute a cause of forfeiture of the appointment.

Each member of the SB can withdraw from the assignment at any time, according to the procedures that will be established in the regulations of the Body.

In the event of forfeiture or withdrawal by one of the members of the SB, the Board of Directors shall promptly replace the member that has become ineligible.

5.5. Activities and powers

The Supervisory Body meets at least four times a year and whenever one of the members has asked the Chairman to convene it, justifying the opportunity of calling a meeting. It may also delegate specific functions to the Chairman. Each meeting of the SB is recorded in minutes.

In order to carry out the assigned tasks, the Supervisory Body is vested with all the powers of initiative and control over all company activities and personnel levels and reports solely to the Board of Directors through its Chairman.

The duties and powers of the Supervisory Body and its members cannot be syndicated by any other corporate body or structure, it being understood that the Board of Directors can verify the consistency between the activity actually carried out by the Body and the mandate assigned to it. In addition, the SB, except for prevailing provisions of law, has free access - without the need for any

prior consent - to all Company Functions and Bodies, in order to obtain any information or data deemed necessary for the performance of its duties.

The Supervisory Body carries out its functions in coordination with the other control bodies or Functions existing in the Company. In addition, the SB liaises with the company functions involved from time to time in all aspects related to the implementation of the Procedures. The SB may also avail itself of the assistance and support of employees and external consultants, in particular for problems that require the help of specialist skills.

The Supervisory Body organises its activities on the basis of an annual action plan, through which the initiatives to be undertaken are planned in order to assess the effectiveness of the Model as well as its updating. This plan is submitted to the Board of Directors.

The Supervisory Body determines its annual budget and submits it to the Board of Directors for approval.

The Supervisory Body, in overseeing the effective implementation of the Model, is endowed with powers and duties that it exercises in compliance with the law and the individual rights of workers and parties concerned, as set out below:

- carry out, also through other persons (e.g., their own consultants), inspection activities;
- have access to all documentation or information relating to the Company's activities, which may be requested from all the Company's personnel, as well as from the Directors, the sole Auditor and suppliers of goods and services of the Company;
- report serious and urgent events to the Board of Directors, as well as any events that make it necessary to amend or update the Model;
- propose the adoption of penalties related to the violation of the Model, as per paragraph 6, to the person with disciplinary power;
- coordinate with the HR function to define training programmes relating to Legislative Decree no. 231/2001 and the Model referred to in paragraph 7;

- prepare, every six months, a written report to the Board of Directors, with the following minimum content:
 - a summary of the activities, checks carried out by the SB during the period and their results;
 - any discrepancies between the Procedures and the Model;
 - reports received on possible violations of the Model and results of checks concerning the above reports, as well as on facts that may constitute offences;
 - disciplinary procedures initiated upon proposal of the SB and any penalties applied;
 - general evaluation of the Model and its effective functioning, with possible proposals for additions and improvements;
 - any changes to the regulatory framework;
 - summary of any expenses incurred;
- report to the sole Auditor, at least annually, on the application of the Model, its functioning, updating and on significant facts or events detected. Specifically, the SB:
 - reports to the sole Auditor any deficiencies found with regard to the organisational structure and the effectiveness and functioning of the Procedures;
 - reports on violations of the Model and on facts that may constitute offences.

The Board of Directors, the Chairman and the Chief Executive Officer have the right to call a meeting of the Supervisory Board at any time. Similarly, the SB has the right, in turn, to request, through the Functions or competent persons, the call of the aforesaid corporate bodies for urgent reasons. Meetings with the bodies to which the SB reports must be recorded in minutes and a copy of the minutes must be kept by the SB and the bodies involved from time to time.

5.6. Information flows to the SB and whistleblowing schemes

The SB must promptly obtain, by way of non-exhaustive example, the following information:

- any illicit conduct (or any conduct that appears to be illicit to the whistleblower) which is relevant pursuant to Legislative Decree no. 231/2001, that the whistleblower has become aware of in the performing of their duties, or any violation (or any conduct that appears to be a violation) of the provisions of the Model, or any conduct that is not compliant with the behavioral rules adopted by the Company;
- critical, abnormal or atypical issues found by the Company's Functions in the implementation of the Model;
- measures and/or information from judicial police bodies, or from any other authority, from which it is apparent that investigations are being carried out, even against unknown persons, for crimes referred to in the Decree committed within the scope of the Company's activity;
- internal and external communications regarding any type of offence that may be connected with the offences referred to in the Decree (e.g., disciplinary measures initiated/implemented against employees);
- requests for legal assistance made by employees in the event of judicial proceedings for offences referred to in the Decree;
- news relating to changes in the organisational structure;
- updates to the organisational system and the system of proxies and powers of attorney (including those relating to the system of powers regarding health and safety at work and environmental safety);
- any communications from the Auditor concerning matters that may indicate deficiencies in the internal control system, reprehensible facts, and observations on the Company's financial statements;
- copy of the minutes of the meetings of the Board of Directors and the determinations of the Sole Auditor.

Such information must be provided to the SB by the Managers of the Company Functions according to their area of competence.



As also provided for by Law no. 179 of 30 November 2017, which introduced whistleblowing into the regulations contained in Legislative Decree no. 231/2001, the Company adopts all the measures necessary to ensure that acts of retaliation or discrimination, direct or indirect, against the whistleblower are prohibited for reasons directly or indirectly linked to the report. In particular, the adoption of discriminatory measures against the whistleblower may be reported to the National Labour Inspectorate, for the measures within its competence, as well as by the whistleblower, also by the trade union organisation indicated by the same. Furthermore, any retaliatory or discriminatory dismissal of the whistleblower shall be considered null and void. The change of duties pursuant to article 2103 of the Civil Code is also null and void, as well as any other retaliatory or discriminatory measure adopted against the whistleblower. It is the responsibility of the employer, in the event of disputes linked to the imposition of disciplinary sanctions, or to de-scanning, dismissal, transfer, or submission of the whistleblower to another organisational measure having direct or indirect negative effects on working conditions, subsequent to the submission of the report, to demonstrate that these measures are based on reasons unrelated to the report itself. Finally, it should be noted that, in the event of reports or reports made in the manner and within the limits of the law, the pursuit of the interest in the integrity of the entity, as well as the prevention and repression of misappropriation, constitutes just cause for disclosure of information covered by the obligation of secrecy referred to in Articles 326, 622 and 623 Criminal Code and article 2105 of the Civil Code (except where the obligation of professional secrecy applies to a person who has become aware of the news as a result of a professional consultancy or assistance relationship with the body, firm or natural person concerned). When news and documents that are communicated to the body delegated to receive them are subject to corporate, professional or official secrecy, disclosure in a manner that exceeds the purposes for which the offence was eliminated and, in particular, disclosure outside the communication channel specifically set up for that purpose, constitutes a breach of the relative obligation of secrecy.

All recipients of the Model must communicate directly with the Supervisory Body, to report any violations of the Model, through confidential internal mail or through a dedicated e-mail.



In compliance with whistleblowing regulation, the Company has also set up two additional information channels to guarantee the confidentiality of the identity of the whistleblower. The report may then be sent by electronic mail or by traditional mail to the Chairman of the Supervisory Board, to the addresses indicated on the Company's website.

Reports may also be anonymous and must describe in detail the facts and persons reported.

Behaviour aimed exclusively at slowing down the activity of the SB is sanctioned.

In any case, the Company protects whistleblowers in good faith against any form of retaliation, discrimination or penalisation for reasons connected, directly or indirectly, with the reporting, without prejudice to the right of the assignees to protect themselves if they are found to be responsible for criminal or civil liability related to false statements and without prejudice to legal obligations. In any case, the confidentiality of the identity of the whistleblower and of the information in any context subsequent to the report itself is guaranteed, without prejudice to legal obligations and the protection of the rights of the Company or of persons accused erroneously or in bad faith. The report is considered to have been made in good faith when it is made on the basis of a reasonable conviction based on facts.

In addition to the reports described above, information must be submitted to the Supervisory Body regarding news concerning disciplinary proceedings and penalties or the measures taken to close such proceedings with their reasons.

The Supervisory Body may submit proposals to the Board of Directors concerning additional types of information that the managers involved in the management of at-risk activities must transmit together with the frequency and methods by which such communications are sent to the Supervisory Board, also through the definition of a specific operating procedure and/or the integration of existing procedures.

Reports received and documentation managed by the SB in general are kept by the SB in a special archive, whether paper or computer, for the entire duration of the Company. The members of the



Board of Directors and the Sole Auditor, as well as persons authorised from time to time by the SB, are allowed access to this archive.

6. Disciplinary system

6.1. General principles

The Decree provides for the introduction of a “disciplinary system to punish noncompliance with the measures set out in the model,” both for persons in a top management position and for persons subject to management and supervision by others.

The existence of a system of penalties applicable in the event of non-compliance with the rules of conduct, provisions and internal procedures set out by the Model is in fact indispensable to guarantee the effectiveness of the Model itself.

By virtue of the provisions of the aforementioned Law no. 179/2017 on whistleblowing and with reference to any recipient of the Model, it should be noted that conduct that may be sanctioned must also include the violation, in any way, of the measures to protect the whistleblower, as well as the performing with malicious intent or gross negligence of reports that prove to be unfounded.

The application of sanctions must remain completely independent from the course and outcome of any criminal or administrative proceedings initiated by judicial or administrative authorities in the case in which the behaviour to be punished also applies to integrate an offense pursuant to Decree or a criminal or administrative offense that is relevant pursuant to legislation on the protection of health and safety in the workplace. In fact, the rules set out by the Model are adopted by the Company in full autonomy, regardless of whether any types of conduct may constitute a criminal or administrative offense and whether judicial or administrative authorities intends to prosecute this offense.

The Supervisory Body is responsible for verifying the adequacy of the disciplinary system, constantly monitoring any procedures for imposing penalties on employees, as well as for

intervening against external parties and also reports any infringements of which it becomes aware in the exercise of its own functions.

6.2. Violations of the Model

Violations of the Model include:

- behaviours that constitute the types of offence contemplated in the Decree;
- conduct that, though not constituting one of the offenses referred to in the Decree, is clearly aimed at committing them;
- conduct that does not comply with the Procedures referred to in the Model and the Code of Conduct;
- conduct that does not comply with the provisions of the Model or referred to in the Model and, in particular, does not comply with the control measures listed in paragraphs 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21 and 22 of the Special Section and with the Procedures referred to in the Model itself;
- Uncooperative behaviours toward the Supervisory Board, consisting in, by way of example and but not limited to, the refusal to provide the required information or documentation, failure to comply with general and specific directives of the Supervisory Board in order to obtain the information it deems necessary for the performance of its duties and absence without justified reason during inspection visits scheduled by the Supervisory Board and failure to attend training meetings;
- breaches of confidentiality obligations or retaliatory or discriminatory acts against those who have reported illegal conduct or a violation of the Model, for reasons directly or indirectly related to the report (including the violation of the anti-retaliatory provisions provided for the whistleblowing legislation);
- performing with malicious intent or gross negligence of reports that prove to be unfounded.

The seriousness of violations of the Model will be assessed on the basis of the following circumstances:

- presence and degree of intent;
- presence and degree of negligent, reckless behaviour;
- the extent of the danger and/or consequences of the violation for the persons covered by the regulations on the protection of health and safety at work, as well as for the Company;
- predictability of the consequences;
- timing and way in which the violation occurs;
- circumstances in which the violation occurs;
- repeat occurrence consisting in repeated imposition of disciplinary sanctions for violations of the Model, as well as in the repetition of behaviours that are relevant from a disciplinary point of view, assessed both in terms of the single event and overall (though not punished).

6.3. Measures against employees

The violation of the individual rules of conduct of this Model, including the violation, in any way, of the measures to protect the whistleblower, or the malicious or grossly negligent making of reports that prove to be unfounded by employees subject to the national collective labour agreement applied by the Company constitutes a disciplinary offence.

Any violation authorises the SB to require the competent company Function to initiate disciplinary proceedings and the possible imposition of one of the penalties listed below, determined on the basis of the seriousness of the violation committed in the light of the criteria indicated in paragraph 6.2 and of the behaviour carried out before (e.g., any previous violations committed) and after the fact (e. g. notification to the SB of the irregularity) by the perpetrator of the violation.

Disciplinary measures that can be imposed against said employees - in compliance with the procedures laid down in article 7, paragraphs 2 and 3, of Law no. 300 of 30 May 1970 (Workers'

Statute) and any special regulations applicable, as well as applicable national collective labour agreement(s) - are those provided for by the following penalties:

- Verbal reprimand;
- Written warning;
- Fine amounting to no more than three hours of pay;
- suspension from service and remuneration for a period not exceeding 3 days;
- Disciplinary dismissal with the right to notice pursuant to the said CCNL and dismissal for cause without notice.

In any case, the penalties applied and/or violations ascertained will always be notified by the competent company function to the Supervisory Board.

In particular, with reference to violations of the Model by employees, it is provided that:

- verbal or written reprimand measures according to the seriousness of the violation shall be taken against an employee who violates the Procedures set forth in the Model or who adopts, when carrying out activities in at-risk activities, conduct in violation of the Model's provisions, unless such conduct results in the application of measures set forth in the Decree;
- a fine is incurred by employees who relapse in any of the violations involving verbal reprimand or written warning referred to in the point above, more than twice within a period of two years, or violate several times internal procedures provided for by this Model on a single occasion or adopt several times behaviours that breach the requirements of Model in the course of the activities of the areas at risk, provided that such conduct does not lead to the application of measures provided for by the Decree;
- suspension from service and remuneration for a period not exceeding three days is incurred by employees who:
 - by violating the procedures provided for by this Model or adopting behaviours that breach the requirements thereof, cause damage to the Company or expose it to an

objective situation of danger, provided that these behaviours are not clearly aimed at committing an offence or result in the application of measures set out in the Decree;

- relapse in a behaviour involving any of the violations that provide for a fine as specified in the paragraph above, more than twice in a period of two years;
- disciplinary dismissal with right of notice in accordance with the applicable national collective labour agreement(s) is incurred by employees who relapse in any of the violations involving suspension referred to in the preceding paragraph point more than twice within a period of two years, after formal written warning; dismissal for just cause without notice shall occur if the employee behaves in a manner which does not conform to the provisions of the Model and is directed solely at committing an offence provided for by the Decree and if employees adopt conduct that blatantly violates the requirements of the Model involving the application by the Company of the measure set out by the Decree or if the employee violates the measures to protect the whistleblower or makes intentional or grossly negligent reports that prove to be unfounded.

Moreover, with reference to the risk of committing offenses that violate regulations concerning occupational health and safety provided for by the Circular of the Ministry of Labour No. 15816 of 11 July 2011 concerning the “*Organisational and Management Model as per Article 30 of Legislative Decree No. 81/2008*”:

- a measure of written warning is incurred by employees who do not comply with the Model in the case where the violation involves the occurrence of a situation of potential danger for the physical integrity of one or more persons including the author of the violation, and provided that one of the cases provided for in the following paragraphs;
- a fine is incurred by employees who relapse in a behaviour in the case of any violations that involve a written warning as referred to in the point above more than two times in a period of two years or who do not comply with the Model, in the case in which the violation involves the occurrence of an injury to the physical integrity of one or more persons, including the

author of the violation, and provided that one of the cases provided for in the following paragraphs;

- suspension from service and remuneration for a period not exceeding three days is incurred by employees who:
 - do not comply with the Model, in the case in which the violation causes injury qualifiable as “serious” to the physical integrity of one or more persons, including the author of the violation, pursuant to article 583, paragraph 1, of the Criminal Code, and provided that one of the cases provided for in the following paragraph;
 - relapse in conduct involving any of the violations that provide for a fine as specified in the paragraph above, more than twice in a period of two years;
- disciplinary dismissal with the right of notice shall be imposed on employees who commit a repeat conduct in any of the violations involving suspension of service and remuneration, as specified in the preceding point, more than twice in a period of two years; employees who do not comply with the Model shall be dismissed for just cause without notice, if the violation causes an injury, which can be qualified as very serious under article 583, paragraph 2, of the Criminal Code, to the physical integrity or death of one or more persons, including the perpetrator of the infringement.

It is understood that the provisions of the Model cannot be interpreted in such a way as to constitute a derogation from the provisions concerning sanctions for unjustified dismissals set out in Article 18 of Law No. 300/1970 as amended by Law No. 92 of 28 June 2012, and by Legislative Decree No. 23 of 4 March 2015.

6.4. Violations of the Model by executives and related measures

With regard to violations of the single rules contained in this Model, including the violation, in any way, of the measures to protect the whistleblower, or the malicious or grossly negligent making of reports that prove to be unfounded committed by Company employees with executive status, these also constitute a disciplinary offence.

Any violation authorises the SB to require the Chairman to impose one of the sanctions listed below, determined on the basis of the seriousness of the violation committed in the light of the criteria indicated in paragraph 6.2 and of the behaviour carried out before (e.g., any previous violations committed) and after the fact (e.g., the communication to the SB of the irregularity) by the perpetrator of the violation.

Disciplinary measures that can be imposed against said executives - in compliance with the procedures laid down in article 7, paragraphs 2 and 3, of Law no. 300 of 30 May 1970 (Workers' Statute) as well as the national collective labour agreement(s) applied and any special regulations applicable - are those provided for by the following penalty system:

- Written reprimand;
- Dismissal for cause with the right to notice;
- Dismissal for cause.

In any case, the penalties applied and/or violations ascertained will always be notified by the competent company function to the Supervisory Board.

In particular, with reference to violations of the Model by executives, it is provided that:

- In the event of a non-serious violation of one or more procedural or behavioural rules provided for in the Model, an executive incurs in a written reprimand consisting in a warning to observe the Model, which constitutes a necessary condition for maintaining a relationship of trust with the Company;
- In the event of non-serious, but repeated violation of one or more procedural or behavioural rules provided for in the Model, the executive will incur in a measure of disciplinary suspension from work and from pay;
- In the case of a serious breach of one or more procedural or behavioural rules provided for in the Model such as to constitute a significant violation, or in the event of a repeat violation involving a disciplinary written reprimand, the executive will incur a measure of justified dismissal with right to notice;

- in the event that the violation of one or more of the procedural or behavioural requirements of the Model is so serious as to irreparably damage the relationship of trust, not allowing the continuation, even temporarily, of the employment relationship, including the event of violation of the measures to protect the whistleblower, or in the event of the malicious or grossly negligent making of reports that prove to be unfounded, the executive will incur a measure of dismissal for cause.

In addition, for employees of the company who hold the position of executive, a serious violation of the Model's requirements is:

- the violation of the obligation of direction or supervision on employees about the correct and effective application of the Model;
- The violation of the obligation of direction and supervision of other employees who, though not linked to the Company by an employment relationship (e.g., self-employed workers, consultants, temporary staff, etc.) are nevertheless subject to the direction and supervision of an executive pursuant to article 5(1)(b) of Legislative Decree No. 231/2001, without prejudice to the nature of the contract with these workers.

It is understood that the provisions of the Model cannot be interpreted in such a way as to constitute a derogation from the provisions concerning sanctions for unjustified dismissals set out in Article 18 of Law No. 300/1970 as amended by Law No. 92 of 28 June 2012, and by Legislative Decree No. 23 of 4 March 2015.

6.5. Measures against members of the Executive Body and the Sole Auditor

In the event of violation of the Model, including the violation, in any way, of the measures to protect the whistleblower, or the malicious or grossly negligent making of reports that prove to be unfounded by one or more members of the Company's Executive Body, the SB will inform the entire Board of Directors and the Sole Auditor that they will take the appropriate measures consistent with the seriousness of the violation committed, in light of the criteria set out in paragraph 6.2 and in accordance with the powers provided for by law and/or the Articles of Association

(declarations in the minutes of meetings, request to convene or calls of the Shareholders' Meeting with appropriate measures on the agenda against those responsible for the violation, etc.).

Disciplinary measures that can be imposed against one or more members of the Executive Body, subject to a resolution of the Board of Directors to be adopted with the abstention of the person concerned and, where provided for by law and/or the Articles of Association, by resolution of the Shareholders' Meeting, are those provided for by the following penalty system:

- Written reprimand;
- Temporary suspension from office;
- Withdrawal from office.

In particular, with reference to violations of the Model committed by one or more members of the Company's Executive Body, it is provided that:

- In the event of a non-serious violation of one or more procedural or behavioural rules provided for in the Model, a member of the Executive Body incurs in a written reprimand consisting in a warning to observe the Model, which constitutes a necessary condition for maintaining a relationship of trust with the Company;
- in the event of a serious violation of one or more procedural or behavioural rules provided for in the Model, the member of the Executive Body is temporarily suspended from office;
- in the event of a serious violation of one or more procedural or behavioural rules provided for in the Model such as to irreparably damage the relationship of trust, including the event of violation of the measures to protect the whistleblower, or in the event of the malicious or grossly negligent making of reports that prove to be unfounded, the member of the Executive Body shall be dismissed from office.

In addition to the members of the Executive Body of the Company, a punishable violation of the Model is also a violation of the obligation of direction or supervision of staff concerning the correct and effective application of the requirements of the Model.

In case of violation of the Model by the entire Executive Body of the Company, the SB will inform the Sole Auditor so that he or she can immediately convene the Shareholders' Meeting for the appropriate measures.

In the event of a violation by the Sole Auditor, inherent to the control function on the adequacy of the organisational, administrative and accounting structure adopted by the Company and on its actual functioning, as provided for by law, the SB will inform the Executive Body which will take the appropriate measures consistent with the seriousness of the violation and in accordance with the powers provided for by law and/or the Articles of Association (declarations in the minutes of the meetings, requests to convene or call of the Shareholders' Meeting with the agenda to discuss adequate measures against the perpetrators of the violation, etc.).

6.6. Measures against members of the SB and third parties

For measures against the members of the SB, reference should be made to the rules for their removal from office (paragraph 5.4).

For measures against third parties, reference should be made to the rules governing relations with them (paragraph 4).

7. Communication of the Model and training of recipients

The external communication of the Model is carried out through the most appropriate means (e.g., the Company's website).

The HR function is tasked operationally with training relating to the Model and the relevant regulations and for this purpose it coordinates itself with the Supervisory Body.

The Company formalises and implements specific training plans, with the aim of ensuring effective knowledge of the Decree, the Code of Conduct and the Model; the contents of training are differentiated according to whether it is aimed at employees as a whole, employees operating in specific risk areas, Directors, etc.



Participation in training is mandatory and participants' attendance is traced.

The training can also take place through the use of IT tools (e.g., in "e-learning" mode) and is carried out with the support of experts in the reference regulations.

SPECIAL SECTION

8. Introduction

As already pointed out in paragraph 3 of the General Section, pursuant to the provisions of article 6, paragraph 1, letter a) of the Decree, the Company has identified the at-risk activities (Control and Risk Self Assessment).

The Company has therefore identified and effectively implemented adequate controls in the control system in order to make it suitable for reducing the risk of commission of offences.

They are indicated below:

- At-risk activities with reference to each category of offence identified as relevant for the Company;
- for each At-risk Activity, the controls in place, aimed at or in any case suitable for reducing the risk of committing the alleged offences. These controls are contained in the Procedures and other parts of the internal control system.

9. Predicate offences relevant to the Company

Considering the structure and activities carried out by the Company, through its control and risk self assessment activities, the Company has identified the following categories of predicate offences as relevant:

- Offences against Public Administration (Articles 24 & 25);
- IT-related felonies and unlawful processing of data (article 24-bis);
- Felonies committed by criminal organisations and transnational crimes (Article 24-ter and article 10 of Law No. 146 of 16 March 2006).
- Felonies against industry and commerce (article 25-bis.1);

- corporate offences, including those of corruption between private persons (article 25-ter);
- Felonies against individual's freedoms (Article 25-quinquies);
- manslaughter or grievous bodily harm through negligence, committed in violation of the rules on health and safety at work (Article 25-septies);
- Handling stolen goods, laundering and use of money, assets or benefits whose origin is illegal (Article 25-octies)
- Felonies regarding breach of copyright (Articles 25-novies);
- Inducements not to make statements or to make false statements to the courts (Article 25-decies);
- Environmental crimes (Article 25-undecies);
- Use of illegally staying third country nationals (Article 25-duodecies).

10. General controls

In addition to the provisions of the Code of Conduct, the following controls apply to the management of all at-risk activities:

- Conduct is prohibited:
 - such as to supplement the types of offences considered above;
 - which, though it is such that it does not in itself constitute a specific type of offence among those considered above, may potentially become so;
 - in any case not in line or not in compliance with the principles and requirements contained in the Model and the Code of Conduct;
- At-risk activities must be managed solely by the competent company functions;



- Company employees must scrupulously abide by, and comply with, any limits set forth in the organisational proxies or powers of attorney granted by the Company;
- Company employees are required to comply with the company procedures applicable to at-risk activities, appropriately updated and disseminated within the organisation.

11. Offences against public administration

11.1. Applicable offences

Considering the structure and activities carried out by the Company, through its control and risk self assessment activities, the Company has identified the following offences against the PA as relevant:

Misappropriation of funds from the State (Article 316-bis of the Criminal Code) consisting in the conduct of whomsoever, outside Public Administration, having obtained grants, subsidies or loans from the State or other public body or from the European Communities intended to favour initiatives aimed at the realization of works or the performance of activities of public interest, do not use them for the aforesaid purposes.

Misappropriation of funds from the state (Article 316-ter of the Criminal Code) consisting in the conduct of whomsoever, unless the act constitutes the offence set out in article 640-bis of the Criminal Code, through the use or presentation of false statements or documents or documents attesting to untrue things, or through the omission of due information, unduly obtains, for themselves or for others, contributions, loans, subsidised mortgages or other disbursements of the same type, whatever denominated, granted or paid by the State, by other public bodies or by the European Communities.

Fraud against the State or other public entity (Article 640, paragraph 2, point 1, of the Criminal Code) consisting in the conduct of whomsoever, by means of trickery or deception, mislead someone into error, procure an unfair profit to the detriment

**Aggravated fraud to obtain public funds
(Article 640-bis of the Criminal Code)**

of others for themselves or others, if the act is committed to the detriment of the State or another public body or on the pretext of having someone exempted from military service.

consisting in the same conduct referred to in the point above if it is committed to obtain subsidies, loans, subsidized mortgages or other funds of the same kind, however denominated, granted and paid by the State, other public bodies or by the European Communities.

Computer fraud against the State or other public entity (Article 640-ter of the Criminal Code)

consisting in the conduct of whomsoever, by altering in whatever way the functioning of a computer or telematic system or intervening without right, by whatever means, on data, information or programmes contained in a computer or telematic system or a system relating thereto, procures for himself or others an unlawful profit to the detriment of the State or other public entity

**Bribery for the performance of an official act
(Article 318 of the Criminal Code)**

consisting in the conduct of a public official who, in order to exercise his/her functions or authority, unduly receives, either for himself/herself or for a third party, money or other benefits or the promise of such

Bribery for the performance of an act in breach of official duties (Article 319 of the Criminal Code)	consisting in the conduct of a public official who receives, for himself or a third party, money or other benefits, or accepts a promise of such money or benefits, in order to omit or delay or for having omitted or delayed an official duty, or in order to perform or for having performed an act contrary to his official duties
Bribery in judicial proceedings (Article 319-ter of the Criminal Code)	consisting in acts of corruption if committed in order to favour or damage a party in civil, criminal or administrative proceedings
Undue inducement to give or promise benefits (Article 319 quater of the Criminal Code)	consisting in the conduct of a public official or person in charge of a public service who, by abusing his position or powers, induces anyone to wrongfully give or promise him or a third party money or other benefits, unless it constitutes a more serious offence, as well as in the conduct of whomsoever gives or promises money or other benefits
Bribery of a public service officer (Article 320 of the Criminal Code)	consisting in conduct referred to in Articles 318 and 319 of the Criminal Code, if committed by a person tasked with a public service
Penalties for the corrupter (Article 321 of the Criminal Code)	pursuant to which the punishments laid down in articles 318, paragraph 1, 319, 319-bis, 319-ter and 320 of the Criminal Code in relation to the cases set out in Articles 318 and 319 of the Criminal Code, apply also to whomsoever give or promise

Incitement to bribery (Article 322 of the Criminal Code)

a public official or person responsible for a public service money or other benefits.

consisting in the conduct of whomsoever offers or promises money or other benefits not due to a public official or a person in charge of a public service for the exercise of his/her functions or powers, or to induce him/her to omit or delay an act of his/her office, or to act contrary to his/her duties, if the offer or promise is not accepted, as well as by in conduct of a public official or a person in charge of a public service who solicits a promise or offer of money or other benefit for the exercise of his/her functions or powers or solicits a promise or the giving of money or other benefits by a private citizen for the purposes set out in Article 319 of the Criminal Code

on the basis of the reference to Article 322-bis made by Article 25, paragraph 4, of Legislative Decree no. 231/2001, the offences referred to in Articles 314, 316, 317 to 320 and 322, third and fourth paragraphs of the Criminal Code apply even if the conduct is directed towards:

- members of the Commission of the European Communities, the European Parliament, the Court of Justice and the Court of Auditors of the European Communities;
- officials and contracted agents within the meaning of the Staff Regulations of officials of the European Communities or the conditions of employment of agents of the European Communities;

- any person seconded to the European Communities by the Member States or by any public or private body, who carries out functions equivalent to those performed by European Community officials or other agents;
- members and employees of bodies created on the basis of Treaties establishing European Communities;
- whomsoever, in other EU Member States, perform functions or activities equivalent to those of Italian public officials and persons in charge of a public service;

judges, prosecutors, deputy prosecutors, officials and agents of the International Criminal Court, persons who are seconded by States Parties to the Treaty establishing the International Criminal Court who perform functions corresponding to those of officials or agents of the International Criminal Court, and members and agents of entities formed on the basis of the Treaty establishing the International Criminal Court. The provisions of Articles 319-quater, second paragraph, 321 and 322, first and second paragraphs, shall also apply if the money or other benefit is given, offered or promised to:

- persons mentioned in the first paragraph of the Article;
- persons exercising functions or activities corresponding to those of public officials and of person in charge of a public service in other foreign States or public international bodies, where the fact is committed to obtain an undue advantage in international business transactions or to obtain or maintain a economic and financial business for oneself or others.

For an example of the possible methods of committing offences, reference should be made to the document “Control & risk self assessment and Gap analysis pursuant to Legislative Decree no. 231/2001.”

11.2. At-risk activities

Considering the structure and activities carried out by the Company, through its control and risk self assessment activities, the Company has identified the following at-risk activities with reference to offences against PA:

- Management of institutional relations with public bodies (at international, national and/or local level);
- Management of relations with Public Administration during inspections (e.g., health and safety in the workplace, environmental, tax, etc.);
- Litigation management (e.g. civil and labour law);
- Management of the commercial activity and participation in tenders/negotiations organised by public bodies or entities ascribable to Public Administration;
- Procurement of goods and services, including procurement and consultancy;
- Management of monetary and financial flows - payments;
- Management of invoices receivable and credit;
- Management of intra-group transactions (e.g. buying and selling of goods/services);
- Selection, recruitment and management of personnel including temporary workers, including management of the incentive and bonus system;
- Management of expense statements and related reimbursements.

11.3. Controls

Below follow the controls in place for each At-risk Activity:

Management of institutional relations with public bodies (at international, national and/or local level)

-
- “high-profile” relationships relating to the at-risk activity in question are normally managed by the General Manager; other persons who deal with public officials are endowed with appropriate powers;

-
- the Office Manager is entrusted with the management of bureaucratic formalities relating to Chinese personnel seconded to Italy by means of specific password access to a dedicated portal;
 - the guidelines for the management of relations with public officials are constituted by the principles provided for by the Code of Conduct;
 - meetings and contacts with Public Administration representatives are reported and traced through the archiving of the related e-mails and/or the formalisation of reports and/or minutes.
-

Management of relations with Public Administration during inspections (e.g., health and safety in the workplace, environmental, tax, etc.)

- The powers for the management of this at-risk activity are vested in the General Manager;
- the different actors involved in the various stages of the process are clearly identified. In particular:
 - in the case of labour law/social security, workplace health and safety and environmental inspections and/or assessments, the involvement of the Office Manager, HR Manager and the Prevention and Protection Service Manager (RSPP) is envisaged;
 - in the event of inspections and/or assessments in administrative/financial matters by the Guardia di Finanzia (Italian Tax Police) and Agenzia delle Entrate (Italian Revenue Agency), the involvement of the Finance Manager is envisaged;
 - these persons are supported by the persons in charge of the functions involved in the inspections, as well as by the Legal Counsel;
 - the General Manager signs the final minutes of the inspection visits;

- inspectors may be provided with appropriate facilities (e.g., segregated rooms, network access, hardware, etc.) at the request of the inspectors;
 - the persons who participate in checks, inspections or audits inform their hierarchical superior and the SB of any critical issues that have emerged during the execution of the assessments, inspections or audits, and communicate to them:
 - identification data of the inspectors (name and entity to which they belong);
 - date and time of arrival of inspectors;
 - duration of the inspection;
 - subject-matter of the inspection;
 - its outcome;
 - any minutes drawn up by the inspection body;
 - a list of any documents submitted;
 - the documentation is kept, by the Functions concerned, in a specific archive, in such a way as to prevent its subsequent modification, in order to allow the correct traceability of the entire process and to facilitate any subsequent controls;
 - the At-Risk Activity in question is governed by a Procedure relating to relations with Public Administration that regulates the rules of conduct, roles and responsibilities, operating procedures, traceability and archiving of minutes and documents.
-

Litigation management (e.g. civil and labour law)

- The powers for the management of this at-risk activity are vested in the General Manager, as well as in the legal representatives appointed by the Company;

-
- the General Manager and legal representatives grant mandates to external professionals tasked with litigation and inform the SB of the initiation of proceedings, of the results of the various phases of the activity, of the conclusion of the proceedings, as well as of any critical issues that may arise during the proceedings;
 - the different persons involved in the various phases of the At-risk Activity in question are clearly identified. In particular:
 - the Legal Counsel selects external consultants and handles disputes with the support of the latter and the Legal Team of ZTE Corporation;
 - following selection by the Legal Counsel and Legal Team of ZTE Corporation, the General Manager and the legal representatives confer the mandate on the legal advisors;
 - each of the parties involved is responsible for the traceability of the requests for information received during the dispute, as well as for the internal evaluation and authorization process of the documentation submitted during the dispute.
-

Management of the commercial activity and participation in tenders/negotiations organised by public bodies or entities ascribable to Public Administration

- The powers for the management of this at-risk activity are vested in the General Manager, as well as in the legal representatives appointed by the Company;
 - the different persons involved in the various phases of the At-risk Activity in question are clearly identified:
 - the Sales Team's specialised Account Manager manages contacts with potential public customers;
-

- meetings with customers are attended by the General Manager, as well as commercial or technical figures;
 - the preparation of the offer is carried out by a Bid Manager (belonging to the Sales Team) appointed from time to time;
 - the offers are processed by the Pre-sales Engineering area for the technical part and by the Commercial area - in concert with ZTE Corporation - for the economic part of the offer;
- During the pre-contractual phase, a duly approved memorandum of understanding may be formalised;
 - the contractual relationships are constantly formalised by means of a written contract drawn up on the basis of a template provided by the Legal Counsel and duly authorized and signed by persons with appropriate powers;
 - the contracts provide for a contractual clause/addendum of commitment to respect the principles of the Model and the Code of Conduct, otherwise the contracts will be terminated;
 - the At-Risk Activity in question is governed by a Procedure governing commercial activities, which sets out the rules of conduct, roles and responsibilities, operating procedures, traceability and archiving of documents.
-

Procurement of goods and services, including tenders and consultancy

- The powers for the management of this at-risk activity are vested in the General Manager, as well as in the legal representatives appointed by the Company;
 - the different persons involved in the various phases of the At-risk Activity in question are clearly identified:
-

- in the case of small purchases, it is the function concerned that directly manages needs by submitting a request for offer to three market participants;
 - in other cases, the purchase request is handled by ZTE Corporation, with particular reference to the selection of subcontractors; this choice is shared with the customer;
- the selection of suppliers is characterised by a systematic evaluation of their integrity requirements;
 - remuneration to suppliers is adequately justified in relation to the type of goods/services provided and is in line with existing market conditions or practices;
 - the contractual relationships are constantly formalised by drafting a written contract drawn up on the basis of a template provided by the Legal Counsel and duly authorised and signed by persons with adequate powers of attorney conferred by the Company;
 - each supplier is required to sign clauses to adhere to the Group's anti-bribery policy and to the principles of the Code of Conduct, as well as to fill in and sign the ZTE Supplier CSR - Letter of Commitment;
 - consultants are chosen in a transparent and non-discriminatory manner, based on the requirements of professionalism, independence and competence and are appointed by persons with adequate powers on the basis of the powers of attorney granted by the Company;
 - consultants shall be appointed in writing, indicating the agreed remuneration and the content of the service;
 - at the end of the assignment, the consultant is requested to provide details in writing of the services rendered;
-

- remuneration of consultants is adequately justified in relation to the type of service/assignment and is in line with existing market conditions or practices or professional tariffs for the category concerned;
 - the documentation is kept, by the Functions concerned, in a specific archive, in such a way as to prevent its subsequent modification, in order to allow the correct traceability of the entire process and to facilitate any subsequent controls;
 - this at-risk activity is governed by the (Transitional) Purchase Bidding Management Regulation for Non-Production Materials (of the Administrative Service Type), Purchase Bidding System Training Course (Non-Production Materials of the Administrative Service Type) and subcontractor procedures.
-

Management of monetary and financial flows - payments

- The powers for the management of the at-risk activity in question are vested in the Chairman of the Board of Directors, the General Manager and a special Attorney;
 - limits are set on the autonomous use of financial resources, by determining quantitative expenditure thresholds, consistent with management skills and organisational responsibilities;
 - the different persons involved in the various phases of the At-risk Activity in question are clearly identified:
 - The Administration function monitors invoices payable and uploads them to the FOL (Group software) system, which assigns a registration number and an identification code for the Company;
 - The Finance Department then carries out a further check and produces a report with payment deadlines;
-

-
- The FOL system provides for various approval steps, involving the Head of the requesting function, the Accounting and Audit departments of ZTE Corporation and the Finance Manager of ZTE Italia;
 - ZTE Corporation is in charge of bank loading for the execution of the payment and carries out bank reconciliations, also monitored by the Finance Manager of ZTE Italia;
- save for situations of necessity and urgency, for which specific compensatory controls are provided, there is no subjective identity between those who commit the Company to third parties and those who authorise or arrange the payment of sums due on the basis of the commitments undertaken;
 - specific reports are to be drawn up and all the authorisation steps are to be recorded in the system;
 - transactions involving the use of economic or financial resources have an express reason and are motivated by the requesting party and are documented and recorded in accordance with the principles of professional and accounting correctness;
 - cash flows are prohibited, except for minimum types of expenditure (petty cash) expressly authorised by the Managers of the Functions involved;
 - with reference to banking and financial transactions, the Company uses only financial and banking intermediaries subject to transparency and correctness regulations in compliance with European Union regulations;
 - payments to third parties are made through banking channels by means that ensure evidence that the beneficiary of the payment is actually the third party contracting with the Company;
 - this at-risk activity is governed by a specific Procedure governing the activities of the Administration and Finance area, which defines the rules of conduct, roles and
-

responsibilities, information flows between ZTE Corporation and ZTE Italia, operating procedures, traceability and archiving of documents with reference to the management of financial transactions.

Management of invoices receivable and credit

- the different persons involved in the various phases of the At-risk Activity in question are clearly identified:
 - the Accounting Department receives invoicing input from ZTE Corporation's Logistics Manager;
 - the relevant Account Manager and Finance Department manage reminders in the event of delays in credit collection;
 - ZTE Corporation periodically carries out bank reconciliations;
 - an ad-hoc system is in place to manage electronically the authorization to issue the invoice with reference to specific customers;
 - this at-risk activity is governed by a specific Procedure governing the activities of the Administration and Finance area, which defines the rules of conduct, roles and responsibilities, information flows between ZTE Corporation and ZTE Italia, operating procedures, traceability and archiving of documents with reference to the management of financial transactions.
-

Management of intra-group transactions (e.g. buying and selling of goods/services)

- The powers for the management of this at-risk activity are vested in the General Manager;
-

-
- all intra-group transactions are formalised as part of the Intercompany Services Framework Agreement, authorised and signed in accordance with the current system of powers;
 - the amounts provided for in intragroup contracts correspond to market criteria;
 - intercompany transactions are recorded through an ad-hoc system managed by the Finance Department of ZTE Corporation;
 - intercompany reconciliations are systematically carried out;
 - reconciliation reports are systematically archived;
 - the at-risk activity in question is governed by a specific Procedure governing the activities of the Administration and Finance area, which sets out the rules of conduct, roles and responsibilities, information flows between ZTE Corporation and ZTE Italia, operating procedures, traceability and archiving of documents with reference to the management of financial transactions, and specifically with regard to intercompany transactions:
 - preparation, control and authorisation of intercompany contracts;
 - management of invoices and intercompany payments;
 - assessment and execution of tax obligations with reference to the purchase and sale of intra-group goods/services (transfer pricing models).
-

**Selection, recruitment and management of personnel including temporary workers,
including management of the incentive and bonus system**

-
- The powers for the management of this At-Risk Activity are vested in the General Manager and Special Attorneys;
 - the different actors involved in the various stages of the process are clearly identified. In particular:
-

- the function concerned request an additional or replacement resource;
 - the Line Manager and HR Manager manage the candidate interview;
 - depending on the job description, the interview can also be managed by the General Manager and Line Manager/HR Manager of the Western Europe area;
 - the General Manager signs the letter of recruitment;
- the onboarding process takes place in the following steps:
- communication by the Function concerned of the resource requirements to the HR Manager;
 - definition of the job description and remuneration range carried out by the HR Manager;
 - approval of the headcount by ZTE Corporation;
 - conducting of a series of evaluation interviews;
 - drawing up of an evaluation form following each interview;
 - contractualisation and inclusion of the selected resource;
- direct or indirect relations between the candidate and PA are verified and evaluated in advance;
- CVs received from candidates and interview files are stored in a paper archive prepared for each person hired by the HR Manager;
- candidate evaluations are formalized in specific documentation, which is guaranteed to be archived by the HR Manager;
- the employment contracts provide for a contractual clause/addendum with the commitment to comply with the principles of the Model and the Code of Conduct;
- with reference to the remuneration of resources:

- pay slips are processed using specific software and with the support of an external consultant;
 - the payroll process is outsourced;
- the incentive scheme is designed on the basis of objective criteria, based on the results achieved;
 - at the beginning of the year, a four-monthly monitoring of the objectives is carried out;
 - communications with which incentives and bonuses are explained to employees are regularly formalised by the HR Manager;
 - the bonus, authorised by the General Manager, is paid by means of a pay slip;
 - the documentation is kept, by the Functions concerned, in a specific archive, in such a way as to prevent its subsequent modification, in order to allow the correct traceability of the entire process and to facilitate any subsequent controls;
 - this at-risk activity is governed by the Procedures “Regulation on New Hire Selection and On-boarding” and “Regulation on Performance Evaluation.”
-

Management of expense statements and related reimbursements

- prior authorisation to travel is granted in writing by the Line Manager;
 - in order to request reimbursement, employees must upload the expense statement to the FOL system, indicating the type of expenses incurred and their description;
 - the FOL system automatically produces a page with barcode that must be printed and delivered to the Administration function with the supporting documents;
 - the payment of the expense statements, by the Finance Department of ZTE Italia and ZTE Corporation, follows the procedure established with reference to payments under the at-risk activity “Management of monetary and financial flows - Payments”;
-



-
- the HR Manager has a corporate credit card that may be used with the prior authorisation of the Finance Manager of ZTE Corporation;
 - this at-risk activity is governed by the document “ZTEIT_Regulation_04 Business Trips”.
-

12. IT-related felonies and unlawful processing of data

12.1. Applicable offences

Considering the structure and activities carried out by the Company, through its control and risk self assessment activities, the Company has identified the following IT-related offences as relevant:

**Forgery of electronic documents
(Article 491-bis of the Criminal
Code)**

consisting in cases of falsehoods, whether material or ideological, committed on public deeds, certificates, authorisations by a representative of Public Administration or by a private party, if they concern a “computer document with probative effect,” i.e., a computer document with at least a simple electronic signature. “Computer document” means the computer representation of acts, facts or data that are legally relevant (such crime extends the criminal prosecution of offences provided for in Book II, Title VII, Chapter III of the Criminal Code to computer documents with probative effect)

**Unauthorized access to a computer
or telecommunications system
(Article 615-ter of the Criminal
Code)**

consisting in conduct of whomsoever unlawfully introduces oneself, i.e., circumventing any form, even minimal, the barriers to entry into a computer or telematic system protected by security measures, or maintains it against the will of those who have the right to exclude it.

**Unauthorized possession and
circulation of access codes to
computer or telecommunications**

consisting in the conduct of whomsoever unlawfully obtains, reproduces, spreads, communicates or gives codes, keywords or other suitable means to access to a computer or telematic system, protected by security

systems (Article 615-quater of the Criminal Code)

measures, or in any case provides indications or instructions suitable for the purpose of obtaining a profit for oneself or others or of damaging others

Distribution of equipment, devices or programs intended to damage or interrupt a computer or telecommunications system (Article 615-quinquies of the Criminal Code)

consisting in conduct of whomsoever, in order to unlawfully damage a computer or telematic system, computer data or programmes contained therein or pertaining thereto, or to contribute to the total or partial interruption or alteration of its functioning, obtains, produces, reproduces, imports, spreads, communicates or in anyway puts at the disposal of others computer equipment, devices or IT programmes

Installation of equipment designed to intercept, prevent or interrupt computer or telecommunications communications (article 617-quinquies of the Criminal Code)

consisting in conduct of whomsoever, except for the cases permitted by law, installs equipment capable of intercepting, preventing or interrupting communications relating to a computer or telematic system or between multiple systems

Damage to computer information, data or programmes (article 635-bis of the Criminal Code)

consisting in the conduct of whomsoever destroys, deteriorates, deletes, alters or suppresses computer information, data or programmes of others, unless the fact constitutes a more serious offense

Damage to information, data or programs used by the state or other public entity or, in any case, of public benefit (Article 635-ter of the Criminal Code)

consisting in the conduct of whomsoever destroys, deteriorates, deletes, alters or suppresses any computer information, data or programmes used by the State or any other public body, or body anyway having a public utility, provided that the act does not constitute a more serious offence

Damage to computer or telecommunications systems (Article 635-quater of the Criminal code)

consisting in conduct of whomsoever, through any of the conducts under Article 635-bis of the Criminal Code, or through the introduction or transmission of data, information or programmes, destroys, damages or makes unusable, either in whole or in part, the computer or telematic systems of others or seriously hampers their functioning, provided that the act does not constitute a more serious offence

Damage to computer or telecommunications systems of public benefit (Article 635-quinquies of the Criminal Code)

consisting in conduct described in the article 635-quater of the Criminal Code, if it is aimed at destroying, damaging, making unusable, in whole or in part, any computer or telematic system of public utility or at seriously hampering their functioning.

Computer fraud by the individual providing electronic signature certification services (article 640-quinquies of the Criminal Code)

consisting in conduct of whomsoever provides electronic signature certification services in order to procure unfair profits for oneself or others or to cause other damage, violates obligations provided for by the law for the release of a qualified certificate

For an example of the possible methods of committing offences, reference should be made to the document “Control & risk self assessment and Gap analysis pursuant to Legislative Decree no. 231/2001.”

12.2. At-risk activities

Considering the structure and activities carried out by the Company, through its control and risk self assessment activities, the Company has identified the following at-risk activities with reference to IT-related offences:

- management of Computer Systems.

12.3. Controls

Below follow the controls in place for each At-risk Activity:

Management of Information Systems

- The software used for business management is standard software downloaded from a specific Group platform;
 - the purchase of licenses for such software is the responsibility of ZTE Corporation;
 - systems are subject to backup policies with servers located in Germany;
 - network security is ensured by the presence of appropriate firewall systems;
 - access to workstations is protected by an alphanumeric password system;
 - security implementation, maintenance and monitoring activities are managed by ZTE Corporation;
 - ZTE Italia avails itself of a consultant with whom a specific contract has been signed for technical support related to wiring, LAN assembly, assistance and installation of company systems;
 - ZTE Corporation operates the ZTE Italia website and its content;
 - traceability of operations performed and related communications between users and IT support from ZTE Corporation is ensured;
 - this at-risk activity is governed by the “IT Security Policy”, which contains instructions for users regarding the correct use of the systems and the security rules to be observed.
-

13. Felonies committed by criminal organisations and transnational offences

13.1. Applicable offences

Considering the structure and activities carried out by the Company, through its control and risk self assessment activities, the Company has identified the following felonies committed by criminal organisations as relevant:

Crime syndicate (Article 416 of the Criminal Code)

consisting in the conduct of whomsoever promotes, establishes and organises an association of three or more persons in order to commit more than one offence and whomsoever participates in it

Mafia-type association (Article 416-bis of the Criminal Code)

punishes whomsoever participates in a Mafia-type association including three or more persons, including whomsoever promotes, direct and organise it. Mafia-type association is said to exist when the participants take advantage of the intimidating power of the association and of the resulting conditions of submission and silence to commit criminal offences, to manage or at all events control, either directly or indirectly, economic activities, concessions, authorizations, public contracts and services, or to obtain unlawful profits or advantages for themselves or for others, or with a view to prevent or limit the freedom to vote, or to get votes for themselves or for others on the occasion of an election. An association is said to be of the armed type when the participants have firearms or explosives at their disposal, even if hidden or deposited elsewhere, to achieve the objectives of the said association. The provisions of article 416-bis of

the Criminal Code also apply to the Camorra and to any other associations, whatever their local titles, even foreign, seeking to achieve objectives that correspond to those of Mafia-type unlawful association by taking advantage of the intimidating power of the association.

Crimes committed using the conditions set forth in article 416-bis of the Criminal Code, i.e., to facilitate the activities of associations as set out in the same article

Inducement to make no declarations or to make mendacious declarations to the judiciary authority (Article 377-bis of the Criminal Code).

consisting in the conduct of whomsoever, by violence or threats, or by offering or promising money or other advantage induces a person summoned to give a statement usable in criminal proceedings before the judicial authority, not to give statement, when such a person has the right to remain silent, unless the act constitutes a more serious offence

Aiding and abetting (Article 378 of the Criminal Code)

consisting in conduct of whomsoever, after committing a crime for which the law establishes the death penalty, life imprisonment or imprisonment, and apart from the cases of conspiracy therein, helps individuals to circumvent investigations of authorities, or to evade the search of the authorities

For an example of the possible methods of committing offences, reference should be made to the document “Control & risk self assessment and Gap analysis pursuant to Legislative Decree no. 231/2001.”

13.2. At-risk activities

Considering the structure and activities carried out by the Company, through its control and risk self assessment activities, the Company has identified the following at-risk activities with reference to felonies committed by criminal organisations and transnational offences:

- Procurement of goods and services, including procurement and consultancy;
- Management of monetary and financial flows - payments;
- Management of intra-group transactions (e.g. buying and selling of goods/services);
- Fiscal management;
- selection, recruitment and management of personnel, temporary workers, including administration of the incentive and bonus system.

13.3. Controls

Below follow the controls in place for each At-risk Activity:

Procurement of goods and services, including tenders and consultancy

The controls are the same as those referred to in paragraph 11.3 of this Special Section and the corresponding At-Risk Activity. Furthermore:

- in the choice of Suppliers, Contractors, and Consultants, orientation towards counterparties that provide the greatest guarantees in ethical, organisational, technical and financial terms is assured (including, but not limited to, ethical qualification elements such as the signing of Legality Protocols, the registration in White Lists established at Prefectures, the request or the achievement of legality rating are duly taken into account);
 - third parties who refuse to provide or otherwise fail to provide such documentation are not selected as contractual counterparties of ZTE Italia;
-

-
- periodic monitoring of Suppliers, Contractors, and Consultants selected through a re-qualification process is carried out.
-

Management of monetary and financial flows - payments

Management of intra-group transactions (e.g. buying and selling of goods/services)

The controls are the same as those referred to in paragraph 11.3 of this Special Section and the corresponding At-Risk Activities.

Fiscal management

-
- The powers for the management of this at-risk activity are vested in the General Manager;
 - the different persons involved in the various phases of the At-risk Activity in question are clearly identified. In particular, tax requirements are managed by the Accounting function, with the support of an external tax consultant: the Accounting function prepares the draft tax calculation (including VAT calculations), the tax consultant verifies the draft and pays taxes;
 - traceability of transactions is guaranteed by the information systems used in company operations, while that of services rendered is attested by the presence and archiving of documents and internal communications;
 - the documentation is kept, by the Accounting function concerned, in a specific archive, in such a way as to prevent its subsequent modification, in order to allow the correct traceability of the entire process and to facilitate any subsequent controls;
 - this At-Risk Activity is regulated by a specific Procedure governing the activities of the Administration and Finance area, which sets out the rules of conduct, roles and responsibilities, information flows with the external tax consultant, operating methods,
-

and traceability and archiving of documents with reference to the management of tax obligations.

**Selection, recruitment and management of personnel including temporary workers,
including management of the incentive and bonus system**

The controls are the same as those referred to in paragraph 11.3 of this Special Section and the corresponding At-Risk Activity. Furthermore:

- during the selection process for recruitment, the integrity criteria of candidates are evaluated;
- candidates are required to submit a self-declaration of pending charges.

With specific reference to the offence of inducement not to make statements or to make false statements to judicial authorities (article 377-bis of the Criminal Code), please refer to paragraph 20.2 of this Special Section.

14. Offences against industry and trade

14.1. Applicable offences

Considering the structure and activities carried out by the Company, through its control and risk self assessment activities, the Company has identified the following offences against industry and trade:

Fraudulent trading (Article 515 of the Criminal Code)

consisting in conduct of whomsoever in the exercise of a commercial activity, or in a shop open to the public, delivers a purchaser a movable thing for another or a movable thing whose origin, provenance, quality or quantity is different from that declared

Manufacturing and sale of goods produced encroaching on industrial property rights (Article 517-ter of the Criminal Code)

constituted by the conduct of whomsoever, being able to know of the existence of the industrial property title, manufactures or uses industrially objects or other goods made by usurping an industrial property title or in violation of it, or of whomsoever, in order to make a profit, introduces into the territory of the State, holds for sale, puts on sale with direct offer to consumers or puts into circulation the aforementioned goods.

For an example of the possible methods of committing offences, reference should be made to the document “Control & risk self assessment and Gap analysis pursuant to Legislative Decree no. 231/2001.”

14.2. At-risk activities

Considering the structure and activities carried out by the Company, through its control and risk self assessment activities, the Company has identified the following at-risk activities with reference to offences against industry and trade:

- management of the commercial activity and participation in tenders/negotiations organised by public bodies or entities ascribable to Public Administration;

- sale of Network System services and products to private individuals;
- sale of mobile device products and provision of after-sales services to private individuals.

14.3. Controls

Below follow the controls in place for each At-risk Activity:

Management of the commercial activity and participation in tenders/negotiations organised by public bodies or entities ascribable to Public Administration

The controls are the same as those referred to in paragraph 11.3 of this Special Section and the corresponding At-Risk Activity. Furthermore:

- with regard to the use of ZTE branded products used in the provision of services by the Company, the information to be provided to potential customers on the characteristics of such products is determined by the ZTE Corporation in accordance with the Group Code of Conduct, which prescribes the principle of accuracy and truthfulness of all information provided to the market on the products and services provided;
 - with reference to the use of non-ZTE branded products used in the provision of services by the Company, the contracts that govern relations with suppliers include specific clauses that guarantee:
 - the correspondence between the characteristics of the products supplied and those laid down in the contracts;
 - indemnification for the Company in the event of violations of third-party rights committed by suppliers regarding the manufacture or use of products;
 - checks are carried out by the Functions concerned to assess the conformity of the characteristics of the products used with those declared by the supplier. The documentation supporting the checks carried out shall be archived.
-

Sale of Network System services and products to private individuals

- The powers for the management of this at-risk activity are vested in the General Manager, as well as in the legal representatives appointed by the Company;
 - the different persons involved in the various phases of the At-risk Activity in question are clearly identified:
 - the Sales Team's specialised Account Manager manages contacts with potential private customers;
 - meetings with customers are attended by the General Manager, as well as commercial or technical figures;
 - the preparation of the offer is carried out by a Bid Manager (belonging to the Sales Team) appointed from time to time;
 - the offers are processed by the Pre-sales Engineering area for the technical part and by the Commercial area - in concert with ZTE Corporation - for the economic part of the offer;
 - During the pre-contractual phase, a duly approved memorandum of understanding may be formalised;
 - the contractual relationships are constantly formalised by means of a written contract drawn up on the basis of a template provided by the Legal Counsel and duly authorized and signed by persons with appropriate powers;
 - with regard to the use of ZTE branded products used in the provision of services by the Company, the information to be provided to potential customers on the characteristics of such products is determined by the ZTE Corporation in accordance with the Group Code
-

of Conduct, which prescribes the principle of accuracy and truthfulness of all information provided to the market on the products and services provided;

- with reference to the use of non-ZTE branded products used in the provision of services by the Company, the contracts that govern relations with suppliers include specific clauses that guarantee:
 - the correspondence between the characteristics of the products supplied and those laid down in the contracts;
 - indemnification for the Company in the event of violations of third-party rights committed by suppliers regarding the manufacture or use of products;
- checks are carried out by the Functions concerned to assess the conformity of the characteristics of the products used with those declared by the supplier. The documentation supporting the checks carried out shall be archived;
- the At-Risk Activity in question is governed by a Procedure governing commercial activities, which sets out the rules of conduct, roles and responsibilities, operating procedures, traceability and archiving of documents.

Sale of mobile device products and provision of after-sales services to private individuals

- The powers for the management of this at-risk activity are vested in the General Manager, as well as in the legal representatives appointed by the Company;
 - the different persons involved in the various phases of the At-risk Activity in question are clearly identified:
 - The Account Manager, Technical Manager and Project Manager prepare the offer;
 - ZTE Corporation sets a pricing basis, to be adjusted during the negotiation phase at local market conditions;
-

- ZTE Corporation gives final approval to the proposal;
 - two agencies manage after-sales services in favour of ZTE Italia;
- the contractual relationships with customers and the said agencies are constantly formalised by means of a written contract drawn up on the basis of a template provided by the Legal Counsel and duly authorized and signed by persons with appropriate powers;
- The information to be provided to prospective customers on the characteristics of mobile devices products is defined by ZTE Corporation in accordance with the Group's Code of Conduct, which prescribes the principle of accuracy and truthfulness of all information provided to the market on the products and services provided;
- checks are carried out to verify:
- the correct correspondence between the description and the technical and commercial information of the product sold and the content of the information material or in any case on any material (including packaging) delivered to customers or used for advertising the product;
 - that the information provided complies with internal and Community regulations and generally with applicable legislation;
- the At-Risk Activity in question is governed by a Procedure governing commercial activities, which sets out the rules of conduct, roles and responsibilities, operating procedures, traceability and archiving of documents.
-

15. Corporate offences, including those of corruption between private persons

15.1. Applicable offences

Considering the structure and activities carried out by the Company, through its control and risk self assessment activities, the Company has identified the following corporate offences as relevant:

False corporate disclosures (Article 2621 of the Civil Code)

consisting in the conduct of directors, general managers, managers in charge of drawing up the company's accounts, statutory auditors and liquidators, who knowingly present untrue significant material facts in the financial statements, reports, or other corporate disclosures for shareholders or the public, in a way that actually misleads others in cases where the economic, equity or financial position of the company or the group that the company belongs to has to be communicated by law, in order to procure wrongful profit for themselves or others

Impediment of control activities (Article 2625 of the Civil Code)

consisting in the conduct of directors who, by concealing documents or with other suitable means, prevent or otherwise hinder the performance of control activities legally attributed to shareholders or other corporate bodies

Unlawful return of capital contributions (Article 2626 of the Civil Code)

consisting in conduct of directors who, except for cases of lawful reduction of share capital, return, even under false pretenses, contributions to shareholders or release them from the obligation to execute them

Unlawful distribution of earnings and reserves (Article 2627 of the Civil Code)

consisting in the conduct of directors who share out profits or advances on profits that have not actually been earned or that should be allocated to reserves pursuant to the law or distribute reserves, including not comprising profits, that may not be lawfully distributed

Operations that would harm creditors (Article 2629 of the Civil Code)

consisting in the conduct of directors who, in breach of the law for the protection of creditors, carry out reductions of the company's share capital, mergers with other companies or demergers, thus damaging creditors

Fictitious capital formation (Article 2632 of the Civil Code)

consisting in the conduct of directors and contributing shareholders who, also in part, fictitiously form or increase the share capital, by the assignment of shares to an extent that is higher as a whole than the share capital amount, reciprocal subscription of shares or company stock, significant overvaluation of the contributions of assets in kind or receivables or the company assets in the event of transformation

Bribery between private individuals (Article 2635, paragraph 3, of the Civil Code)

consisting in the conduct of whomsoever offers, promises or gives money or other benefits not due to the directors, general managers, managers in charge of drawing up the company's financial reports, auditors and liquidators, to those who, within the company's organisational framework, exercise management functions other than those of the persons indicated, as well as to those who are subject to the management or supervision of said persons, in order for them to

Incitement to bribery between private individuals (Article 2635-bis of the Civil Code)

perform or omit acts in violation of the obligations inherent to their office or the obligations of loyalty

consisting in the predicate conduct, if the offer or promise of undue money or other benefits is not accepted

Obstructing the operations of public supervisory authorities (Article 2638 of the Civil Code)

consisting in the conduct of directors, general managers, managers responsible for preparing the company's accounting documents, statutory auditors and liquidators of companies or entities and other persons subject to public supervisory authorities by law, or required to meet obligations towards them which, in communications to the aforementioned authorities required by law, in order to hinder the exercise of supervisory functions, expose material facts that do not correspond to the truth, even though they are subject to assessments, on the economic and financial situation of those subject to oversight, or for the same purpose, they conceal by other fraudulent means, in whole or in part, facts which they should have communicated, concerning the same situation, even if the information concerns assets owned or managed by the company on behalf of third parties; or by the fact committed by the directors, general managers, statutory auditors and liquidators of companies, or bodies and other persons subject by law to public supervisory authorities or under obligations towards them, which, in any case, deliberately hinder

their functions, also by omitting communications to the said authorities

For an example of the possible methods of committing offences, reference should be made to the document “Control & risk self assessment and Gap analysis pursuant to Legislative Decree no. 231/2001.”

15.2. At-risk activities

Considering the structure and activities carried out by the Company, through its control and risk self assessment activities, the Company has identified the following at-risk activities with reference to corporate offences:

- Litigation management (e.g. civil and labour law);
- sale of Network System services and products to private individuals;
- sale of mobile device products and provision of after-sales services to private individuals;
- management of relations with the Shareholder and the sole Auditor;
- preparation of the financial statements and communications to the Shareholder or the public relating to the economic, equity or financial situation of the Company;
- transactions relating to share capital: management of contributions, corporate assets, profits and reserves, transactions on equity investments and capital;
- Procurement of goods and services, including procurement and consultancy;
- Management of monetary and financial flows - payments;
- Management of invoices receivable and credit;
- Management of intra-group transactions (e.g. buying and selling of goods/services);
- Selection, recruitment and management of personnel including temporary workers, including management of the incentive and bonus system;
- Management of expense statements and related reimbursements.

15.3. Controls

Below follow the controls in place for each At-risk Activity:

Litigation management (e.g. civil and labour law)

Procurement of goods and services, including tenders and consultancy

Management of monetary and financial flows - payments

Management of invoices receivable and credit

Management of intra-group transactions (e.g. buying and selling of goods/services)

**Selection, recruitment and management of personnel including temporary workers,
including management of the incentive and bonus system**

Management of expense statements and related reimbursements

The controls are the same as those referred to in paragraphs 11.3 and 13.3 of this Special Section and the corresponding At-Risk Activities.

Sale of Network System services and products to private individuals

Sale of mobile device products and provision of after-sales services to private individuals

The controls are the same as those referred to in paragraph 14.3 of this Special Section and the corresponding At-Risk Activities.

Management of relations with the Shareholder and sole Auditor

-
- the different persons involved in the various phases of the At-risk Activity in question are clearly identified:
-

-
- the Accounting function (Finance Manager) is involved in the audits carried out by the sole Auditor on accounting issues;
 - the General Manager manages relations with the Shareholder;
- the traceability of the activities attributable to the process in question is guaranteed by the documentation requested and produced for the Shareholder and the sole Auditor and the related minutes;
- the transmission of data and information, as well as any communication or evaluation expressed by the Shareholder or sole Auditor, are always documented and archived by the competent function.
-

Preparation of the financial statements and communications to the Shareholder or the public relating to the economic, equity or financial situation of the Company

-
- the different persons involved in the various phases of the At-risk Activity in question are clearly identified. In particular:
- A dedicated team of ZTE Corporation draws up the audit report in the ERP system;
 - ZTE Italia's Finance Manager, with the support of an external consultant, revises the audit report;
 - the external consultant deposits the financial statements;
 - the HR Manager acts as corporate secretariat, convenes the Board of Directors and Shareholders' Meeting on behalf of the Chairman and prepares minutes;
- draft financial statements and other accounting documents are made available to the Directors in reasonable time before the meeting of the Board of Directors called upon to resolve on the approval of the financial statements;
-

-
- this At-Risk Activity is governed by a specific Procedure governing the activities of the Administration and Finance area, which sets out the rules of conduct, roles and responsibilities, information flows between ZTE Corporation and ZTE Italia, operating procedures, traceability and archiving of documents with reference to the management of financial statements and preparation of financial statements.
-

Transactions relating to share capital: management of contributions, corporate assets, profits and reserves, transactions on equity investments and capital

- the different subjects involved in the various phases of the At-Risk Activity in question (the Chairman of the Board of Directors, the General Manager, the Finance Manager) are clearly identified;
 - decisions on transactions involving share capital are approved by the Board of Directors and Shareholders' Meeting, after a decision has been taken by the Company's ownership structure, on the basis of the Company's Articles of Association and current statutory regulations;
 - the supporting documentation is kept, by the Functions concerned, in a specific archive, in such a way as to prevent its subsequent modification, in order to allow the correct traceability of the entire process and to facilitate any subsequent controls.
-

16. Felonies against individual's freedoms

16.1. Applicable offences

Considering the structure and activities carried out by the Company, through its control and risk self assessment activities, the Company has identified the following felonies against individual's freedoms as relevant:

Illicit intermediation and labour exploitation (article 603-bis of the Criminal Code)

punishes, for each recruited worker, whosoever:

- 1) recruits labour for the purpose of employment with third parties under exploitative conditions, taking advantage of workers' state of need;
- 2) uses, hires or employs labour, including through the intermediary activity referred to above, subjecting workers to conditions of exploitation and taking advantage of their state of need.

The existence of one or more of the following conditions is considered to be an indicator of exploitation:

- 1) the repeated payment of wages in a way that is manifestly different from the national or territorial collective agreements concluded by the most representative trade unions at national level, or in any case disproportionate to the quantity and quality of the work performed;
- 2) repeated infringement of the legislation on working time, rest periods, weekly rest periods, compulsory leave and holidays;

3) the existence of violations of occupational health and safety rules;

4) subjecting the worker to working conditions, surveillance methods or degrading housing conditions

For an example of the possible methods of committing the offence, reference should be made to the document “Control & risk self assessment and Gap analysis pursuant to Legislative Decree no. 231/2001.”

16.2. At-risk activities

Considering the structure and activities carried out by the Company, through its control and risk self assessment activities, the Company has identified the following at-risk activities with reference to offences against individual’s freedoms:

- Procurement of goods and services, including procurement and consultancy;
- selection, recruitment and management of personnel, temporary workers, including administration of the incentive and bonus system.

16.3. Controls

Below follow the controls in place for each At-risk Activity:

Procurement of goods and services, including tenders and consultancy

The controls are the same as those referred to in paragraphs 11.3, 13.3 and 15.3 of this Special Section and the corresponding At-Risk Activity. Furthermore:

- the selection phase of Suppliers and Contractors is based on transparency criteria, paying the utmost attention to information regarding third parties with whom the Company has
-

contractual relations that may even only give rise to the suspicion of the commission of the offence referred to in this Special Section;

- in the case of the signing of contracts and subcontracting contracts, it is verified that the counterpart's legal requisites of regularity are met, through the delivery and/or acquisition of the documentation required by law (e.g. single document for the regularity of contributions - DURC);
- contracts with Suppliers and Contractors include the Contractor's express obligation, as well as any subcontractors, to comply with:
 - national or territorial collective agreements concluded by the most representative trade unions at national level, or collective agreements of any applicable level;
 - legislation on working time, rest periods, weekly rest periods, compulsory leave and holidays;
 - occupational health and safety rules;
- agreements with Suppliers, Contractors and any subcontractors provide for the commitment of such parties to guarantee the existence of the conditions of legality for the stipulation of employment contracts with employees and the right of the Company to request further documentation or to carry out other checks aimed at ascertaining compliance by the Supplier, Contractor and any subcontractor with the regulations indicated in the previous paragraph;
- correspondence between the names of the workers employed declared by contractors and subcontractors and the workers actually present in the places where they carry out activities on behalf of the Company is verified.

**Selection, recruitment and management of personnel including temporary workers,
including management of the incentive and bonus system**

The controls are the same as those referred to in paragraphs 11.3, 13.3 and 15.3 of this Special Section and the corresponding At-Risk Activity. Furthermore:

- when hiring employees or using temporary or seconded workers, the HR function verifies compliance with labour law regulations and any trade union agreements for hiring and the employment relationship in general;
 - in the case of staff employed through an employment agency, the HR function verifies that it has obtained the authorization to carry out the activity required by the reference regulations;
 - the HR function also verifies the correct classification of personnel in the light of the reference collective agreements and, on the basis of the badge system and with the help of special software, the working hours, rest periods and holidays of staff;
 - the supporting documentation is kept, by the HR function concerned, in a specific archive, in such a way as to prevent its subsequent modification, in order to allow the correct traceability of the entire process and to facilitate any subsequent controls.
-

17. **Manslaughter and serious or very serious injuries committed in violation of occupational health and safety protection regulations**

17.1. **Applicable offences**

Considering the structure and activities carried out by the Company, through its control and risk self assessment activities, the Company has identified the crimes of manslaughter and serious or very serious culpable personal injury committed in violation of the regulations on health and safety at work as relevant:

Manslaughter (committed as an infringement of health and safety at work regulations) (article 589 of the Criminal Code)

punishes whomsoever causes the death of a person by fault with violation of the regulations for the prevention of accidents at work.

Culpable personal injury (committed in violation of the rules on health and safety protection at work) (article 590 of the Criminal Code)

punishes whomsoever culpably causes personal injury to others with violation of the rules for the prevention of accidents at work. In order for the personal injury to be criminally relevant, it must result in illness in the body or mind; the injury is:

- serious, if (alternatively) the result is an illness that endangers the life of the injured person, an illness or an inability to carry out ordinary tasks for more than forty days, the permanent weakening of a sense or organ;
- very serious, if (alternatively) the result is an illness that is certainly or probably incurable, the loss of sense, the loss of a limb, a mutilation that renders the limb useless, the loss of the use of an organ or the ability to procreate, a

permanent and serious difficulty of speech, the deformation or scarring of the face.

For an example of the possible methods of committing offences, reference should be made to the document “Control & risk self assessment and Gap analysis pursuant to Legislative Decree no. 231/2001.”

17.2. At-Risk Activities; the provisions of article 30 of Legislative Decree no. 81 of 9 April 2008

With reference to offences relating to health and safety at work, the Model sets out a different and additional control system from that provided for by accident prevention legislation, and differs from a mere risk assessment.

The Model’s objectives are to control the operating system, in order to ensure its continuous verification and effectiveness, and the Model itself is addressed both to persons exposed to the danger of injury and to those who, throughout the corporate structure, are exposed to the risk of committing culpable crimes, so as to allow the latter to adopt predetermined operational and decision-making standards to avoid death and injuries.

The Model therefore constitutes a second-level control system, which regulates the way in which the safety system must be implemented and controlled and is aimed at avoiding accidents (function already performed by the safety management system), as well as that persons with management responsibilities are subject to offences (in point, see Court of Trani-Molfetta, 11 January 2010).

The Model, therefore, regulates activities at risk of offence, other than those at risk of accident (identified by the Risk Assessment Document and regulated by the safety management system). These activities are identified on the basis of the foregoing and the provisions of article 30 of Legislative Decree no. 81/2008, which lists the areas with reference to which the Model must regulate legal obligations.

At-Risk Activities with reference to the offences of manslaughter and serious or very serious culpable personal injury committed in violation of the regulations on health and safety at work are as follows:

- identification of employer and proxies; appointments and assignment of roles and responsibilities;
- updating of regulations;
- risk assessment and preparation of follow-up measures;
- organisational activities, such as emergencies, first aid, tenders, periodic meetings;
- health surveillance;
- information and training;
- acquisition of documentation and certification;
- supervision, control and audit.

17.3. Controls

Below follow the controls in place for each At-risk Activity:

Identification of employer and proxies; appointments and assignment of roles and responsibilities

-
- The persons referred to in the legislation on health and safety at work are identified and appointed, and they are given the powers - possibly including those of expenditure - necessary to carry out the role;
 - the Employer has delegated part of his powers pursuant to article of 16 Legislative Decree no. 81/2008; some powers and responsibilities have been further sub-delegated to the Regional Managers;
-

-
- the persons referred to in the previous point possess adequate and effective skills in this field, as well as any technical and professional requirements provided for by law;
 - the appointment or, in any case, the attribution of responsibility takes place on a certain date, in writing.
-

Regulatory update

-
- Compliance with the relevant regulations (laws, technical standards and regulations, etc.) is ensured by means of:
 - regulatory updating, carried out by the Prevention and Protection Service Manager, who indicates the need to comply with applicable regulations;
 - periodic monitoring of compliance with the applicable legislation.
-

Risk assessment and preparation of follow-up measures

-
- The Employer is supported by the Prevention and Protection Service and other actors of the safety management system;
 - the risk assessment is contained in a Risk Assessment Document (DVR), specific to all Company premises, drawn up on the basis of a document produced by ZTE Corporation and adapted to Italian legislation;
 - the DVR has attachments relating to ZTE Italia's offices and external activities (commissioning);
 - the Rome site of ZTE Italia is certified according to the OHSAS 18001 standard;
 - the identification of the measures resulting from the risk assessment is carried out on the basis of pre-defined criteria and considers the following aspects:
-

-
- routine and non-routine tasks;
 - activities of all persons having access to the workplace (including external actors);
 - human conduct;
 - external hazards;
 - hazards associated with operations or created in the surrounding environment;
 - infrastructure, equipment and materials at the workplace;
 - changes made to processes and/or the management system, including temporary changes, and their impact on operations, processes and activities;
 - any applicable legal requirements for risk assessment and implementation of the necessary control measures;
 - design of work environments;
 - identification of the activities for which provision should be made for the use of personal protective equipment;
 - definition of criteria for the selection of personal protective equipment;
 - the procedures for delivery of personal protective equipment.
-

Organisational activities, such as emergencies, first aid, tenders, periodic meetings

-
- situations that may cause a potential emergency are identified;
 - emergency management modes are defined;
 - activities to verify the effectiveness of emergency management and emergency simulations are planned and recorded;
-

-
- emergency procedures are updated in the event of accidents or negative results of checks or simulations;
 - the persons in charge are formally identified;
 - emergency and first-aid team personnel are identified, appointed and trained in accordance with the law;
 - exercises are carried out and recorded;
 - regular meetings are held on the basis of a schedule;
 - the technical and professional requirements of contractors are checked (through verification of registration with the Chamber of Commerce and compliance with insurance and social security obligations);
 - interference risk assessment is carried out and formalised in the Single Interference Risk Assessment Document (DUVRI);
 - ZTE Italia also draws up the DUVRI prepared by the customer to whom its employees are assigned (commissioning staff);
 - in the case of activities carried out construction sites, the Safety and Coordination Plan (PSC) prepared by the client is sent by ZTE Italia to subcontractors;
 - subcontractors forward the Operational Safety Plans (POS) to ZTE Italia and these - together with its own - are sent by the Company to the client.
-

Health surveillance

-
- the Company's Occupational Physician is responsible for verifying the suitability of workers for the tasks to be assigned;
-

-
- the Occupational Physician sets out the health surveillance protocol to be submitted to workers and implements health surveillance based on a schedule;
 - the documentation on health surveillance is filed with the HR function.
-

Information and training

-
- All personnel receive appropriate information about the proper manner of performing their duties, are trained and, in the cases provided for by law, are trained;
 - training is provided based on a schedule;
 - training is differentiated according to the level and task of the workers, as well as documented and traced;
 - the training documentation is archived by the HR function.
-

Acquisition of documentation and certification

-
- the certifications are provided to ZTE Italia by the owners of the properties where the Company has its registered office, and are verified based on a schedule.
-

Supervision, control and audit

-
- specific audit activities are planned and conducted based on a specific schedule by the Prevention and Protection Service Manager and the H&S Manager, also with the collaboration of competent corporate persons or external consultants;
 - the audits conducted by the H&S Manager are also carried out on the work of the Prevention and Protection Service Manager;
 - audits are also carried out in relation to the work of subcontractors.
-

18. **Receiving, laundering and using money, goods or benefits of unlawful provenance, including self-laundering**

18.1. **Applicable offences**

Considering the structure and activities carried out by the Company, through its control and risk self assessment activities, the Company has identified the offences of receiving stolen goods, money laundering and the use of money, goods or utilities of illegal origin, as well as self-money laundering as relevant:

Receiving stolen goods (Article 648 of the Criminal Code) consisting in the conduct of whomsoever, apart from participation in the offence, acquires, receives or conceals money or goods which are the proceeds of a criminal offence, or assists in acquiring, receiving or concealing such money or goods, with a view to gain for himself or another

Money laundering (Article 648-bis of the Criminal Code) consisting in the conduct of whomsoever, apart from participation in the offence, substitutes or transfers money, goods or assets obtained by means of intentional criminal offences, or seeks by any other means to conceal the fact that the said money, goods or assets are the proceeds of such offences

Using money, assets or benefits of illegal origin (Article 648 of the Criminal Code) consisting in the conduct of whomsoever, apart from participation in the offence and from the cases as per articles 648 and 648bis, uses money, goods or assets obtained by means of a criminal offence for economic or financial activities

Self-laundering (Article 648-ter.1 of the Criminal Code) consisting in the conduct of whomsoever, having committed or helped perpetrate a crime committed

with criminal intent, uses, replaces, or transfers the money, assets or other assets derived from the commission of said offense into economic, financial, entrepreneurial or speculative assets in order to actually prevent identification of the criminal origin

For an example of the possible methods of committing offences, reference should be made to the document “Control & risk self assessment and Gap analysis pursuant to Legislative Decree no. 231/2001.”

18.2. At-risk activities

Considering the structure and activities carried out by the Company, through its control and risk self assessment activities, the Company has identified the following at-risk activities with reference to offences of receiving stolen goods, money laundering and the use of money, goods or utilities of illegal origin, as well as self-money laundering:

- preparation of the financial statements and communications to the Shareholder or the public relating to the economic, equity or financial situation of the Company;
- transactions relating to share capital: management of contributions, corporate assets, profits and reserves, transactions on equity investments and capital;
- Procurement of goods and services, including procurement and consultancy;
- Management of monetary and financial flows - payments;
- Management of invoices receivable and credit;
- Management of intra-group transactions (e.g. buying and selling of goods/services);
- Fiscal management;
- Management of expense statements and related reimbursements.

18.3. Controls

Below follow the controls in place for each At-risk Activity:

Preparation of the financial statements and communications to the Shareholder or the public relating to the economic, equity or financial situation of the Company

Transactions relating to share capital: management of contributions, corporate assets, profits and reserves, transactions on equity investments and capital

The controls are the same as those referred to in paragraph 15.3 of this Special Section and the corresponding At-Risk Activities.

Procurement of goods and services, including tenders and consultancy

The controls are the same as those referred to in paragraphs 11.3, 13.3, 15.3 and 16.3 of this Special Section and the corresponding At-Risk Activity. Furthermore:

- error indicators are identified to determine any “at-risk” or “suspicious” transactions with counterparties based on:
 - subjective profile of the counterparty (e.g., existence of criminal records, questionable reputation, admissions or statements by the counterparty regarding its involvement in criminal activities);
 - conduct of the counterparty (e.g., ambiguous behaviour, lack of data required for the execution of transactions or reluctance to provide such data);
 - geographical location of the counterparty (e.g., off-shore transactions);
 - economic and financial profile of the transaction (e.g., unusual transactions by type, frequency, timing, amount, and geographical location);
-

- characteristics and purposes of the transaction (e.g., use of names, changes in standard contractual conditions, purpose of the transaction).
-

Management of monetary and financial flows - payments

Management of invoices receivable and credit

Management of intra-group transactions (e.g. buying and selling of goods/services)

Management of expense statements and related reimbursements

The controls are the same as those referred to in paragraphs 11.3, 13.3 and 15.3 of this Special Section and the corresponding At-Risk Activities.

Fiscal management

The controls are the same as those referred to in paragraph 13.3 of this Special Section and the corresponding At-Risk Activity. Furthermore:

- All legislative and regulatory provisions, including regulations, governing compliance with fiscal requirements, also with reference to tax consolidation and transfer pricing rules, where applicable, as well as all circulars, instructions and resolutions issued by the competent public authorities (Agenzia delle Entrate, Ministry of Finance, etc.) are complied with;
 - the deadlines relating to tax obligations are monitored;
 - relations with consultants involved in the at-risk activity in question are formalised by means of a contract, duly authorised and signed by persons with adequate powers on the basis of the proxies conferred by the Company.
-

19. Offenses relating to the infringement of copyright

19.1. Applicable offences

Considering the structure and activities carried out by the Company, through its control and risk self assessment activities, the Company has identified the following offences relating to the infringement of copyright:

Article 171-bis of Law no. 633 of 22 April 1941 consisting in conduct of whomsoever illegally duplicates, for profit, computer programmes or, for the same purpose, imports, distributes, sells, holds for commercial or entrepreneurial purposes or leases programmes contained in media not marked by the Italian Society of Authors and Publishers (SIAE); uses any means intended to permit or facilitate the arbitrary removal or circumvention of software protections; in order to make a profit, reproduces, transfers, distributes, communicates, presents or demonstrates publicly the contents of a database on media without SIAE mark, extracts or reuses the database, distributes, sells or leases a database

Article 171-ter of Law no. 633/1941 consisting in the conduct of whomsoever - among other things - illegally duplicates, reproduces, or distributes literary, dramatic, scientific or didactic, musical or dramatic-musical and multimedia works in the public domain.

For an example of the possible methods of committing offences, reference should be made to the document “Control & risk self assessment and Gap analysis pursuant to Legislative Decree no. 231/2001.”

19.2. At-risk activities

Considering the structure and activities carried out by the Company, through its control and risk self assessment activities, the Company has identified the following at-risk activities with reference to breach of copyright:

- management of Computer Systems.

19.3. Controls

Below follow the controls in place for each At-risk Activity:

Management of Information Systems

The controls are the same as those referred to in paragraph 12.3 of this Special Section and the corresponding At-Risk Activity. Furthermore:

- periodic checks are carried out on installed software and mass storage of systems in use to check for the presence of unlicensed software.
-

20. Inducement to make no declarations or to make mendacious declarations to the judiciary authority

20.1. Applicable offences

The offence of inducing not to make statements or to make false statements to the Judicial Authority is considered potentially applicable to the Company:

Inducement to make no declarations or to make mendacious declarations consisting in the conduct of whomsoever, by violence or threats, or by offering or promising money or other advantage induces a person summoned to give a

to the judiciary authority (Article 377-bis of the Criminal Code)

statement usable in criminal proceedings before the judicial authority, not to give statement, when such a person has the right to remain silent, unless the act constitutes a more serious offence

20.2. At-risk activities; controls

The case referred to in article 377-bis of the Criminal Code is not related to specific business activities.

Therefore, with reference thereto, at-risk activities and corresponding controls to be implemented in the Procedures are not identifiable.

The prevention of this type of offence is therefore constituted by the principles contained in the Company's Code of Conduct, with particular reference to the principles relating to relations with judicial authorities.

21. Environmental offences

21.1. Applicable offences

Considering the structure and activities carried out by the Company, through its control and risk self assessment activities, the Company has identified the following environmental offences as relevant:

Environmental pollution (Article 452-bis of the Criminal Code)	consisting in conduct of whomsoever, in violation of law, causes a significant and measurable impairment or deterioration: 1) of water, air or extensive or significant portions of soil or subsoil; 2) of an ecosystem, biodiversity, including agricultural, flora or wildlife;
Intentional offences against the environment (Article 452-quinquies of the Criminal Code)	consisting in conduct of whomsoever commits the crime of environmental pollution and the offence of intentional environmental disaster;
Organized activities for illegal waste trafficking (Article 452-quaterdecies of the Criminal Code)²	punishes whomsoever engages in the sale, receipt, transportation, export or import or otherwise abusive management of large quantities of waste through several operations and the establishment of continuous organisational means and activities;

² The offence was introduced by Legislative Decree No. 21 of 1 March 2018 and replaces art. 260 of Legislative Decree No. 152/2006, which was abrogated. As specified, in fact, by Article 8 of the Legislative Decree of 1 March 2018, “*from the date of entry into force of this decree, references to the provisions repealed by Article 7, wherever present, shall be considered to refer to the corresponding provisions of the Criminal Code*”.

Unauthorised waste management activities (Article 256 of Legislative Decree No. 152/2006)	consisting in conduct of whomsoever carries out collection, transport, recovery, disposal, trade and brokerage of waste without the required authorization, registration or communication;
Illegal waste trafficking (Article 259 of Legislative Decree No. 152/2006)	consisting in conduct of whomsoever carries out the illegal trafficking of waste under the law.

For an example of the possible methods of committing the offence, reference should be made to the document “Control & risk self assessment and Gap analysis pursuant to Legislative Decree no. 231/2001.”

21.2. At-risk activities

Considering the structure and activities carried out by the Company, through its control and risk self assessment activities, the Company has identified the following at-risk activities with reference to environmental offences:

- management of environmental obligations.

21.3. Controls

Below follow the controls in place for each At-risk Activity:

Management of environmental obligations

- ZTE Italia relies on external suppliers for waste management:
 - for the disposal of packaging materials, the CONI consortium is used;

- for the disposal of waste electrical electronic equipment (WEEE), batteries, USB sticks, mobile phones, and routers, it relies on the ECORIT consortium;
 - for the disposal of office waste, the company relies on the printer supplier (and to a lesser extent ECORIT);
- relations with suppliers are formalised in specific contracts duly signed by persons with suitable powers;
 - ZTE Italia transmits the data required by current legislation electronically to the CONI consortium;
 - with reference to waste disposed of by ECORIT, ZTE Italia submits annually a specific statement on the government website dedicated to the quantity and types of waste produced;
 - this declaration is digitally signed and transmitted by the OHSAS Manager/Office Manager after hearing the Logistic Manager of ZTE Corporation;
 - The Logistic Manager of ZTE Corporation fills out an ad-hoc register to monitor waste management in Italy;
 - with reference to dismantling activities, the Company uses suppliers of environmental services that are subject to a qualification process based on the documentation proving the legal requirements; this documentation is archived;
 - ZTE Italia systematically carries out checks and audits on the disposers it uses.

22. Use of foreign citizens illegally present in the country

22.1. Applicable offences

Considering the structure and activities carried out by the Company, through its control and risk self assessment activities, the Company has identified the following offences related to the use of foreign citizens illegally present as relevant:

Use of illegally staying third country nationals (Article 22, paragraph 12-bis of Legislative Decree no. 286 of 25 July 1998)

consisting in conduct of whomsoever, acting as an employer, employs foreign workers who do not have the residence permit referred to in this Article, or whose permit has expired and for which renewal has not been requested within the period required by law, or has been revoked or cancelled, if the workers employed are (either):

- more than three;
- minors of non-working age;
- subject to the other particularly exploitative working conditions identified in the third paragraph of Article 603-bis of the Criminal Code, in relation to the work to be performed and the working conditions.

For an example of the possible methods of committing the offence, reference should be made to the document “Control & risk self assessment and Gap analysis pursuant to Legislative Decree no. 231/2001.”

22.2. At-risk activities

Considering the structure and activities carried out by the Company, through its control and risk self assessment activities, the Company has identified the following at-risk activities with reference to the offence related to the use of foreign citizens illegally present:

- Procurement of goods and services, including procurement and consultancy;
- selection, recruitment and management of personnel, temporary workers, including administration of the incentive and bonus system.

22.3. Controls

Below follow the controls in place for each At-risk Activity:

Procurement of goods and services, including tenders and consultancy

The controls are the same as those referred to in paragraphs 11.3, 13.3, 15.3, 16.3 and 18.3 of this Special Section and the corresponding At-Risk Activity.

Selection, recruitment and management of personnel including temporary workers, including management of the incentive and bonus system

The controls are the same as those referred to in paragraphs 11.3, 13.3, 15.3 and 16.3 of this Special Section and the corresponding At-Risk Activity. Furthermore:

- in the case of recruitment of third-country nationals already in possession of a residence permit, the existence and validity of the residence permit shall be verified, together with any further documentation needed to perfect their recruitment;
 - in the case of recruitment of third-country nationals already in possession of a residence permit, the HR Manager provides for:
 - the personal request for authorisation (authorisation of recruitment) to be submitted to the competent Prefecture office;
 - giving the authorization, once issued, to the person to be hired, so that s/he can request the competent offices for the issue of entry visa for reasons of employment and therefore, following entry into Italy, the residence permit;
-

-
- obtaining the residence permit or the copy of the application for a residence permit submitted to the post office and the receipt thereof and to file this documentation together with the employment contract;
 - communications required by law to the Centre for Employment and other competent bodies, ensuring that the information transmitted is truthful, complete and based on appropriate documentation;
- the HR function:
- monitors the expiry dates of residence permits and any renewals for third-country workers recruited;
 - verifies, during the employment relationship, that the foreign worker has submitted an application for renewal of the residence permit (of which the worker must produce a copy of the receipt issued by the post office at which the application was made), close to the expiry of its validity and in any case not later than sixty days from it;
- employees hired by ZTE Italia are required to undertake to transmit any communication, letter and request from the competent authorities and offices (Police Headquarters, Prefecture, Employment Centre) regarding the validity or expiry of the residence permit to the company;
- the at-risk activity in question is covered by the Procedures “Regulation on New Hire Selection and On-boarding” and “Regulation on Performance Evaluation” which govern, among other things, the management of formalities relating to the regularity of stay of non-EU personnel, with particular reference to personnel on secondment from China (with reference to the verification, renewal, application for a residence permit, visa and letters of invitation).
-