The Chief Legal Officer

"International Compliance Program" Group Policy

Annex "General Control Standards, Areas at Risk and Specific Standards of Conduct"

TABLE OF CONTENTS

INTRODUCTION

This document identifies the General Control Standards, the Areas at Risk and the Specific Standards of Conduct for each Area of Compliance identified in the scope of the International Compliance Program, as specified below:

a) Corruption crimes;
b) Other crimes against Public Administrations;
c) Accounting fraud;
d) Tax crimes;
e) Organised crime;
f) Financing of terrorism and so-called money laundering crimes;
g) Market abuse;
h) Crimes against individuals;
i) Health and safety crimes;
j) Environmental crimes;
k) Computer crimes;
l) Copyright crimes;
m) Smuggling;
n) Crimes against cultural heritage.

GENERAL CONTROL STANDARDS

The General Control Standards set out below are universally applicable to all Areas of Compliance, and every Foreign Company is required to comply with them:

- *Segregation of duties and responsibilities:* ensuring the segregation of duties between those executing, controlling and/or authorizing figures, also by profiling users within IT systems, in accordance with delegated and proxy powers;
- *Roles and responsibilities:* formalising internal regulations describing tasks, responsibilities and operational methods for carrying out relevant/operational activities;
- *Delegated and proxy powers system:* defining a system of delegated and proxy powers that identifies, consistently with the organisational position and hierarchical level of the recipients, the level of autonomy, power of representation and spending limits assigned;

- *Traceability and storage*: ensuring the traceability and verifiability of activities and controls by means of appropriate documentary and/or IT support, and their storage in compliance with current regulations and Group policies;
- *Impartiality and absence of conflicts of interest*: ensuring that the persons involved in the Areas at Risk described in this document operate with professionalism and impartiality, in compliance with applicable laws and regulations, avoiding and promptly reporting any situation from which a conflict of interest may arise;
- *Correct management of relations with Third Parties*: in relations with Third Parties, according to a risk-based approach, ensuring the following:

  (i) verification of the reliability, reputation and suitability of Third Parties with whom each Foreign Company intends to establish a professional and business relationship;

  (ii) provision of specific contractual instructions requiring Third Parties to comply with the principles contained in this International Compliance Program;

  (iii) verification of the services rendered and appropriateness of the amounts to be disbursed.

AREAS AT RISK AND SPECIFIC STANDARDS OF CONDUCT

Below are the Areas at Risk and Specific Standards of Conduct that each Foreign Company is required to comply with for each Compliance Area.

CORRUPTION CRIMES

For the definition of Corruption Crimes, identification of Areas at Risk and Specific Standards of Conduct, please refer to FS Group Anti-Corruption Policy.

OTHER CRIMES AGAINST PUBLIC ADMINISTRATIONS

The commission of this type of crime presupposes the establishment of relations with public bodies. For the purposes of the International Compliance Program, a 'public body' is typically considered to be any body with a legal status, entrusted with the care of public interests, and which carries out legislative, judicial or administrative activities by virtue of public law and authoritative acts, or which is primarily financed by, or subject to the management and control of state, regional or local authorities, or other public law bodies.

These crimes mainly concern fraud against public bodies and occur when a company carries out one or more unlawful actions or schemes to defraud a public body in order to obtain an economic advantage through false or fraudulent representations, promises or pretences.

This kind of crime is often related to public financing, subsidies and tenders and occurs when a company applies for public financing or subsidies it is not entitled to, or uses them improperly and differently from

what is indicated in the application, or provides the public body with untrue information in order to obtain the award of the tender in the preparation of documents or data for participation in public tendering procedures for the award of a service.

AREAS AT RISK

In relation to this type of crime, the following Areas at Risk are to be monitored:

a) participation in procedures for the awarding of public procurement and concession contracts;
b) performance of procedures for the awarding of public procurement and concession contracts;
c) applications for public funding, subsidies, grants or guarantees issued by public bodies;
d) management of public funding, grants or guarantees obtained;
e) management of relations with public authorities (e.g. with reference to health, safety and environmental requirements, personnel management, payment of taxes).

SPECIFIC STANDARDS OF CONDUCT

Relations with public bodies must be inspired by principles of fairness, professionalism, loyalty and full cooperation, ethics, integrity, transparency and compliance with applicable laws, and must be maintained by the company structures formally delegated and/or by persons formally authorised to do so.

In compliance with the main Specific Standards of Conduct set out in FS Group Anti-Corruption Policy, to which reference should be made, the Foreign Companies shall refrain, in particular, from:

- providing public bodies with information or delivering documents with inaccurate, incorrect, incomplete and/or false content;
- using sums received from public bodies, such as funds, grants or loans, for purposes other than those for which they were intended;
- behaving in a reticent or deceptive manner that could lead the public party into error, also by omitting any due information, in order to direct decisions in favour of Group Companies or Third Parties.

ACCOUNTING FRAUD

Accounting fraud is the intentional manipulation of financial statements to create a false representation of a company's economic and financial situation (e.g. a company may falsify its financial statements by overstating revenues or assets, failing to record expenses and understating liabilities).

Accounting fraud can take place for a variety of reasons to the benefit of the company, including but not limited to:

- continuing to obtain a bank loan in the absence of the necessary requirements;

- declaring non-existent profits or conceal losses;
- concealing circumstances that could adversely affect the company;
- omitting material facts that could mislead interested parties;
- disguising the creation of slush funds.

AREAS AT RISK

In relation to this type of crime, the following Areas at Risk are to be monitored:

a) drafting of documents to be issued to shareholders or to the public (e.g. annual financial statements, periodic financial reports) concerning the economic or financial situation of a Foreign Company, even if such documents are different from those prepared for the purposes of periodic accounting reporting;
b) management of accounting records;
c) management of monetary and financial flows;
d) managing of relations with external auditors.

SPECIFIC STANDARDS OF CONDUCT

In compliance with the main Specific Standards of Conduct set out in the Group's Administrative and Accounting Directives and Procedures, to which reference should be made, the Foreign Companies shall refrain, in particular, from engaging in the following:

- representing or transmitting false, inaccurate, or incomplete data, or, in any case, from data that do not correspond to the true economic, capital and financial situation of the Company, when drafting and representing the company in financial statements, reports or other corporate communications required by law;
- omitting or altering relevant data and information on the economic and financial situation of the Company to be used in financial statements, reports or other corporate communications required by law;
- engaging in conduct that, through the concealment of documents or the use of other fraudulent measures, materially prevents or in any case obstructs the performance of control or auditing activities of the company management by shareholders, the Board of Statutory Auditors or equivalent body or external auditors.

Every operation or transaction of the Foreign Company should be correctly and promptly recorded in the Company's accounting system, in accordance with the criteria indicated by law and the applicable accounting standards.

Every operation and transaction of the Foreign Company should be verifiable, legitimate, consistent and congruous.

In order for the accounts to meet the requirements of truthfulness, completeness and transparency, adequate and complete supporting documentation of the activity performed must be kept for each transaction to allow the following:

- an accurate and complete representation of the company's economic transactions;
- the immediate determination of the characteristics and reasons underlying the transaction;
- the easy formal and chronological reconstruction of the transaction;
- internal controls and audits by the external auditor.

Each accounting entry must faithfully reflect the information contained in the supporting documentation. Therefore, each employee will be responsible for ensuring that supporting documentation is readily available and in order.

TAX CRIMES

Tax crimes may be broadly defined by each jurisdiction to cover a wide range of activities and may occur for a variety of reasons to the benefit of the Company, including but not limited to:

- issue of documents for non-existent transactions;
- failure to register for tax purposes or keeping of incorrect records;
- non-payment, including by offsetting undue claims;
- submission of a false tax declaration;
- tax evasion or refunds through fraud or illegal practices;
- intentional tax reductions by using false and/or fictitious documents (including e.g. invoices);
- obstruction of a Tax Authority Officer.

AREAS AT RISK

In relation to this type of crime, the following Areas at Risk are to be monitored:

a) management of corporate taxation;
b) management of accounting records and documentation to be kept for tax purposes;
c) management of the collection, storing, recording and issuing of invoices or other documents to be kept for tax purposes;
d) collection and evaluation of the accounting data needed to prepare financial statements;
e) management of tax returns;
f) management of activities relating to the settlement and payment of taxes.

SPECIFIC STANDARDS OF CONDUCT

In compliance with the Ferrovie dello Stato Italiane Group's Tax Strategy, to which reference should be made, each Foreign Company should:

- comply with all regulations and, more generally, applicable tax provisions;
- adopt a conduct based on the principle of utmost caution;
- ensure that the tax burden is correctly determined and reported in the tax returns, in accordance with the applicable law and the instructions provided by tax authorities;
- maintain correct, complete and transparent records and books to ensure that they reflect the company's operations;
- monitor deadlines and tax compliance, as well as the transposition of new tax regulations;
- carry out regular update/training activities for those involved in the tax definition/control processes.

ORGANISED CRIME

Organised crime refers to a form of associated crime entailing a stable organisation of several persons for the purpose of committing several crimes. The term "organised crime" also refers to large-scale complex criminal activities carried out by organised groups of persons, in an undefined manner or with complex structures, with the aim of obtaining profits for its participants at the expense of the community and its members.

AREAS AT RISK

In relation to this type of crime, the following Areas at Risk are to be monitored:

a) personnel selection, recruitment, management and incentives;
b) selection of economic operators for the awarding of works, services and supplies;
c) management of relations with Third Parties;
d) extraordinary corporate transactions and/or financial investment transactions and/or use of the Company's own liquidity;
e) investment activities and joint venture agreements or other forms of partnership with local or foreign counterparts.

SPECIFIC STANDARDS OF CONDUCT

With regard to the Areas at Risk identified, each Foreign Company should strictly refrain from:

- establishing business relations or engaging in donations with Third Parties, if there is a well-founded suspicion that such Third Parties may be members of organised crime networks;
- meeting demands of any kind contrary to the law or associating with others for the purpose of committing

multiple offences;

- associating with Third Parties, by providing its own, Third-Party or the Company's knowledge or means to such association, in order to engage in conduct, acts or operations not in line with the provisions set forth herein, the company procedures and the Group's Code of Ethics, or which, in any case, may constitute a crime, albeit only potentially.

Furthermore, for the implementation of the above-mentioned principles of conduct:

- the process of selection of economic operators for the awarding of works, services and supplies must be inspired by the principles of transparency, equal access, professionalism, reliability and cost-effectiveness;
- every transaction should be carried out through the banking system, and customers should be required to make payments exclusively through this system, which allows traceability of financial transactions;
- every operation, including those of an extraordinary nature, within the Group to which it belongs (transformations, mergers, de-mergers, etc.) must be authorised, verifiable, legitimate, consistent and congruous, as well as properly recorded;
- constant monitoring of the company's financial flows (also in relation to the management of intercompany payments) should be carried out;
- specific controls to be carried out on the counterparty must be established and implemented in order to verify the counterparty's identity, registered office, legal nature, reputation and reliability, also with reference to its presence on any national and international Reference Lists and Black Lists for the prevention of money laundering, terrorist financing and organised crime.

FINANCING OF TERRORISM AND SO-CALLED MONEY LAUNDERING CRIMES

Terrorist financing is defined as the provision or collection of funds — by any means, either directly or indirectly — with the intention of using them to support terrorist acts or organisations.

For the purposes of the International Compliance Program, the phenomenon of so-called money laundering can comprise three different types of conduct: (i) conversion or transfer of funds known to be of illicit origin; (ii) concealment or disguise of the true nature, source, location, ownership of, or other rights in or to property known to be of illicit origin; (iii) acquisition, possession or use of property known to be of illicit origin upon receipt.

When the proceeds of a crime are created by the same person who conceals their illicit origin, such conduct is punished in some countries as self-laundering. Money laundering and terrorist financing often have similar transactional characteristics, mostly related to concealment.

Those who engage in money laundering activities send illicit funds through legal channels to conceal their criminal origin, while those who finance terrorism transfer funds that may be of legal or illicit origin in such a way as to conceal their source and their ultimate use, i.e. support for terrorism.

This type of conduct may occur for the benefit of a company, including but not limited to:

- obtain proceeds or any other advantage from illegal activities carried out by the terrorist organisations that have been financed (other advantages may consist in the protection of business in countries where these organisations are quite influential);
- disguise the illegal origin of the proceeds of crime.

AREAS AT RISK

In relation to this type of crime, the following Areas at Risk are to be monitored:

a) contractual relationships with economic operators entrusted with works, services and supplies, partners and other legal entities controlled directly or indirectly by the above-mentioned entities, having their residence or registered office in a country representing a high-risk and non-cooperative jurisdiction;
b) management of monetary and financial flows.

SPECIFIC STANDARDS OF CONDUCT

In order to avoid any possible conduct aimed, even indirectly, at facilitating crimes such as receiving stolen goods, money laundering and the use of money, goods or any other utility of illicit origin, the financing of terrorism, as well as any improper use of financial instruments and/or operations aimed at concealing the origin of the Company's funds, each Foreign Company should:

- use the banking system to carry out transactions, and require customers to make payments exclusively through this system, which allows the traceability of financial movements, refraining from suggesting or accepting any payments 'off the books', i.e. to accounts in Countries other than that of the registered office/residence or in countries indicated in the contract;
- use company credit cards, prepaid cards and/or other payment instruments appropriately and in accordance with the Company's purposes, taking care to safeguard and protect the relevant data;
- keep all data on business counterparties up to date in order to allow a valid assessment of their business profiles;
- refrain from doing business with natural or legal persons known or suspected to belong to criminal or otherwise illegal organisations;
- ensure that every operation, even of an extraordinary nature, within the relevant Group (transformations, mergers, de-mergers, etc.) is authorised, verifiable, legitimate, consistent and congruous, as well as properly

recorded;

- comply with the rules for a correct, complete and transparent recording of accounting entries related to the Company management;
- constantly monitor cash flows in accordance with the different activities carried out within the Company's operations;
- identify the personnel in charge of credit card management, the criteria for allocating company credit cards, and the procedures for using them;
- establish and implement specific controls to be carried out on the counterparty in order to verify its identity, registered office, legal nature, reputation and reliability, also regarding its presence on any national and international Reference Lists and Black Lists for the prevention of money laundering, terrorist financing and organised crime.

MARKET ABUSE

Market abuse can refer to various behaviours, such as:

- possession of inside information in order to carry out or induce others to carry out transactions (purchases, sales, etc.) involving financial instruments;
- disclosure of such inside information to others;
- dissemination of false information in order to cause a significant change in the price of financial instruments;
- engagement in sham transactions or other devices to cause a significant change in the price of financial instruments.

Such conduct may be intended to benefit a company for a variety of reasons, including, but not limited to:

- lowering the price of a target company's financial instruments prior to an acquisition;
- weaken the reputation of a competing company;
- altering the price of a particular financial instrument in the portfolio before engaging in any trading activity related to it.

AREAS AT RISK

In relation to this type of crime, the following Areas at Risk are to be monitored:

a) management of information disclosed to the public (relations with investors, financial analysts, rating agencies, journalists and other mass media representatives, including the management of advertising campaigns; organisation of and participation in meetings of any kind, with the aforementioned parties);
b) management of inside information capable of affecting the performance of listed financial instruments

(e.g. information closely related to new services and markets, accounting data for the period, forecast data and quantitative objectives relating to the performance of operations, communications relating to mergers/de-mergers and new initiatives of particular significance or negotiations and/or agreements relating to the acquisition and/or disposal of significant assets, M&A activities);

c) drafting of accounting documents and prospectuses to be disclosed to the public by law or by company decision;

d) any type of transaction relating to the financial instruments in the portfolio.

SPECIFIC STANDARDS OF CONDUCT

In compliance with the Group's regulatory instruments on Market Abuse, to which reference is made, each Foreign Company is expressly required to refrain from:

- disclosing privileged information to Third Parties, except in cases where such disclosure is required by law or regulations, by Judicial or Administrative Authorities, by provisions or by specific contractual agreements, if such information is aimed at favouring or otherwise obtaining an advantage for the Foreign Company;
- recommending or inducing Third Parties to make purchases, sales or other transactions on financial instruments on the basis of inside information (obtained from company representatives by virtue of their position within the Group or from Third Parties by virtue of their business relations with the Group), if the execution of such transactions is aimed at favouring or in any case obtaining an advantage for the Foreign Company;
- communicating or disseminating, through any communication channel, false or misleading inside data or information on financial instruments, or news whose truthfulness is not certain, likely to alter the value of a financial instrument;
- carrying out transactions that may provide false signals on the value of a financial instrument, so as to induce other traders to take actions capable of producing further price changes.

CRIMES AGAINST INDIVIDUALS

Crimes against individuals may be committed by recruiting, hiring and employing workers in exploitative conditions and taking advantage of their state of need. Furthermore, crimes against individuals may include all actions that violate respect for people and human rights in all their forms, including ethnic, cultural, religious, racial and gender differences.

The existence of one or more of the following conditions may constitute an indicator of exploitation for the benefit of the Company:

- repeated compensation in a manner manifestly different from that specified by law or in any case disproportionate to the quantity and quality of the work performed;
- repeated violation of laws on working hours, breaks, holidays and compulsory leave;
- violations of occupational health and safety regulations;
- subjection of workers to degrading work conditions, surveillance methods or housing situations.

AREAS AT RISK

In relation to this type of crime, the Areas at Risk are as follows:

a) selection, recruitment and management of personnel, with particular regard to the determination of working hours, remuneration, health and safety impacts and working conditions in general;

b) assignment of activities involving the use of Third-Party labour for the provision of labour and/or services, including with regard to economic operators operating in Countries where individual rights are not fully protected by international or local law.

SPECIFIC STANDARDS OF CONDUCT

Foreign Companies are required to comply with the following principles:

- verify, for the direct recruitment of staff, compliance with the labour law when it comes to the recruitment process and the employment relationship in general;
- require economic operators awarding labour, service and supply contracts and their subcontractors to comply with any applicable international and local legislation on forced labour, protection of child and women labour and sanitary conditions;
- establish and implement specific controls on the counterparty in order to verify its reputation and reliability;
- protect the moral and personal integrity of individuals by providing working conditions that respect individual dignity and a safe and healthy working environment;
- ensure the utmost respect for people and human rights in all their forms, including respect for ethnic, cultural, racial and religious differences.

HEALTH AND SAFETY CRIMES

Health and safety crimes mainly concern the failure to comply with local laws and workplace standards suitable to ensure the prevention of accidents and illnesses in the workplace, including fatal ones or those resulting in serious or very serious injuries to employees, committed in violation of occupational health and safety regulations.

Such conduct may occur to a company's advantage for a number of reasons, including but not limited to:

- a reduction of costs resulting from the failure to adopt the necessary safety measures to ensure health and safety in the workplace;
- an increase in productivity, since the performance of work activities without taking into account precautionary procedures and policies could speed up work processes.

AREAS AT RISK

In relation to this type of crime, the following areas should be deemed as risky:

a) compliance with applicable health and safety regulations.

SPECIFIC STANDARDS OF CONDUCT

All Foreign Companies must adopt appropriate occupational health and safety management systems to control their risks in this regard, always taking into account the safety of workers at every stage of the activity and adopting all measures deemed necessary to protect the physical and moral integrity of their workers, Third Parties and communities in which the Company operates, promoting an effective culture of safety protection in the workplace aimed at fostering awareness of the risks and responsibilities of personal behaviours.

In particular, the occupational health and safety management system adopted and effectively implemented by Foreign Companies should:

- consider compliance with legal provisions on health and safety of workers in the workplace as a priority;
- eliminate the risks to the health and safety of workers at the source and, where this is not possible, reduce them to a minimum by means of acquired knowledge and technological progress;
- constantly carry out specific risk assessment activities, also in order to assess the introduction of consequent prevention and protection measures;
- in the case of concessions or subcontracted works, services or supplies by the Company, inform the contractors of the risks present in the working environments in which they are to operate;
- monitor and analyse each occupational accident that occurs, in order to identify any deficiencies in the health and safety management system and to identify any corrective actions to be taken;
- carry out regular information and training activities for employees;
- carry out checks to ensure the application and effectiveness of work safety procedures and instructions by workers and contractors.

In order to maintain an adequate monitoring of the Areas at Risk, each Foreign Company shall allocate organisational, instrumental and economic resources to ensure, on the one hand, full compliance with current

legal provisions on the prevention of accidents at work and, on the other hand, the continuous improvement of the health and safety situation at work, also through the implementation and updating of the relevant prevention measures.

ENVIRONMENTAL CRIMES

Environmental crimes include unlawful acts that cause damage to the environment. These crimes relate to a broad list of illegal activities, such as crimes against wildlife, the illegal trade and disposal of hazardous substances, and many other types of conduct that could harm the environment.

For instance, such crimes could be committed in the following activities:

- management of waste collection, storage, transport and disposal activities, also by outsourcing the activities to Third Parties;
- management of emissions from industrial activities;
- operation and maintenance of plants/devices using environmentally harmful substances.

Environmental crimes could be committed in the interest of a company for a number of reasons, including:

- to reduce the costs resulting from not taking the necessary measures to protect the environment;
- to increase productivity, as doing business without considering environmental issues could speed up the production process.

AREAS AT RISK

In relation to this type of crime, the following areas should be monitored as they are considered at risk:

a) compliance with applicable environmental laws, including during the design, construction, operation and maintenance of infrastructure;
b) selection of Third Parties to carry out specific activities that may have an impact on the environment (e.g. waste management and disposal).

SPECIFIC STANDARDS OF CONDUCT

All Foreign Companies, within the scope of their activities, should prioritize respecting and protecting the environment, especially through:

- the assessment of potential risks and the development of appropriate prevention programmes to protect the environment and public safety;
- the establishment of specific procedures in accordance with the existing environmental legislation;
- the dissemination within the Company of information on environmental protection, promoting awareness

on the issue and ensuring that activities are carried out in compliance with applicable laws;

- the adoption of appropriate means to prevent their activities from causing any form of damage and harm to the ecosystem.

COMPUTER CRIMES

Computer crimes encompass a wide range of activities involving all areas of the company. In general, these crimes can be divided into two categories: (i) crimes that target a computer network or device; (ii) crimes facilitated by the use of computer networks or devices.

The computer crimes considered in this document consist in, for instance: (i) the unauthorised intrusion into a protected computer network; (ii) the introduction of viruses into a computer system; (iii) the interception of data from a computer network; (iv) the interruption of a computer system by damaging, deleting, altering or suppressing computer data; (v) the unlawful interference with the operation of a computer system; (vi) computer fraud and fraudulent use of computer data in order to obtain an unfair financial advantage.

Computer crimes can be committed in the interest of a company for a number of reasons, including the following:

- to gain access to the trade secret of a competing company;
- to obtain confidential information on the market strategies of competing companies;
- to endanger or damage the computer system of a competing company;
- to compromise critical computer systems of a competitor, such as those related to essential infrastructure or production, to cause significant damage.

AREAS AT RISK

In relation to this type of crime, the following should be considered Areas at Risk:

a) business activities carried out using any IT tool (e.g. the e-mail system);
b) management and protection of workstations, laptops, mobile phones and storage devices;
c) definition of the physical and logical security measures to be taken on the computer system, including the classification and processing of information and data and the management of system administrator profiles;
d) activities to secure corporate networks, including encryption of communications and defence against network attacks, which are essential to prevent unauthorised access and data compromise.

SPECIFIC STANDARDS OF CONDUCT

As a general principle of prevention applicable to all business processes at risk of computer crimes being committed, all Foreign Companies must ensure that access to and processing of data contained in computer systems is carried out in compliance with the applicable legal provisions.

Foreign Companies must ensure periodic monitoring, in accordance with applicable local law, of the activities carried out by personnel on the company's computer system, in order to detect unusual behaviour and potential vulnerabilities in the company's systems.

Moreover, Foreign Companies must carry out awareness-raising campaigns, also through specific training sessions where necessary, on the importance of a correct and appropriate use of the IT tools in use within the company's activities.

With regard to the use and management of computer systems, tools, documents or data, Foreign Companies must comply with the following control principles:

- compliance with IT security management procedures;
- preparation and implementation of a corporate policy for managing and monitoring the physical security of IT environments and resources;
- adoption of specific measures to ensure the separation of roles in the change management process (new developments, evolutionary maintenance, corrective maintenance and routine maintenance) of IT systems (application or basic software, hardware and systems);
- provision and implementation of disaster recovery processes and mechanisms to ensure the recovery of specific systems and data in the event of temporary unavailability or permanent loss;
- adoption of specific measures to ensure that the use of assets that may be covered by intellectual property rights complies with legal or contractual provisions;
- implementation of a protection system suitable for identifying and authenticating previously authorised users accessing a processing or transmission system;
- provision of technological tools and levels of protection against spam, spyware, malware, etc.;
- activation of appropriate filters to prevent access to sites that are not relevant to work or that are prohibited;
- revocation of authorisation to use a computer system/application upon termination of employment, change of company role or as a consequence of prolonged non-use;
- implementation of advanced monitoring solutions of network traffic and user activities on computer systems, including the use of anomaly detection systems and detailed user activity logs, in order to detect unusual behaviour, suspicious activities or unauthorised access;

- performance of periodic IT security audits to assess the effectiveness of the security measures implemented, identify potential vulnerabilities and make ongoing improvements;
- performance of regular security tests and simulated attacks to assess the organisation's preparedness, identify weaknesses and improve incident response.

COPYRIGHT CRIMES

Copyright infringement may consist of the use of works protected by copyright law and intellectual/industrial property law without authorisation, i.e. in violation of certain exclusive rights vested in the owner of the copyright and/or intellectual/industrial property right, such as the right to reproduce, distribute, display or perform the protected work, or to make derivative works from it.

AREAS AT RISK

In relation to this type of crime, the following Areas at Risk are to be monitored:

a) the installation, operation, use and reproduction of software protected by copyright and/or intellectual/industrial property law within the company's computer systems;
b) use of texts, images, music and videos protected by copyright and/or intellectual/industrial property law within the company's computer systems;
c) management of intellectual and industrial property rights in relation to trade marks, patents, inventions, designs and utility models.

SPECIFIC STANDARDS OF CONDUCT

Foreign companies take appropriate technical, physical and organisational measures in order to avoid:

- any unlawful use or dissemination to the public, including through computer networks or through connections of any other kind, of the original work protected by copyright and/or intellectual/industrial property law or part thereof;
- the use for business purposes of assets protected by acquired rights in circumvention of the obligations imposed by copyright and/or intellectual/industrial property law or in a manner not intended by the owner;
- the illegal downloading of any software without adequate supporting contractual documentation.

In addition, when a Foreign Company enters into a contract with external contractors for the performance of activities that could potentially be considered at risk of copyright/proprietary rights infringement, such contract must include clauses requiring the contractor to comply with applicable laws and regulations on the

subject.

SMUGGLING

Smuggling occurs when a natural or legal person removes, or attempts to hide goods of foreign origin to avoid paying the relevant border duties. In general terms, smuggling consists of illegally importing or exporting goods in violation of the customs provisions and laws of a state that prohibit or tax their entry, exit and movement.

AREAS AT RISK

In relation to this type of crime, the following Areas at Risk are to be monitored:

a) customs compliance management (preparation and transmission of documentation required by law, management of relations with customs authorities, also with the support of Third Parties, etc.);
b) payment of customs duties and delivery of documents relating to the import/export of materials to customs authorities;
c) selection of economic operators supplying goods and negotiation, conclusion and management of related contracts;
d) warehouse management.

SPECIFIC STANDARDS OF CONDUCT

In addition to the provisions of the FS Group Sanction Policy to which reference is made, Foreign Companies must:

- ensure that all activities and operations are carried out in strict compliance with the relevant regulations;
- define operational procedures for carrying out, either directly or indirectly, customs operations and related monitoring.

CRIMES AGAINST CULTURAL HERITAGE

Crimes against cultural heritage consist of all crimes concerning cultural heritage as a collective legal asset or common property, protected not only from a strictly private-material point of view, but also and above all as a value in itself, for that public component that represents a tool of culture functional to the intellectual education of all individuals.

For example, the following crimes may be included in the category of crimes against cultural heritage:

- dispersal (e.g., theft and misappropriation of cultural property);
- illegal circulation (e.g. violations related to the disposal, illegal import and export of cultural property);

- forgery (forgery of private documents relating to cultural property and forgery of works of art);
- concealment of illicit origin (receiving and laundering of cultural property);
- destruction (destruction, dispersal, deterioration, defacement and unlawful use of cultural or environmental assets, devastation and looting of cultural or environmental assets).

AREAS AT RISK

In relation to this type of crime, the following Areas at Risk are to be monitored:

a) management of cultural heritage, both movable and immovable.

SPECIFIC STANDARDS OF CONDUCT

All Foreign Companies must:

- comply with the regulations protecting cultural and environmental heritage, in particular by setting in place all appropriate controls and activities to safeguard the heritage itself;
- contribute to the fulfilment of all regulatory obligations, including those relating to the acquisition and circulation of cultural goods, or otherwise necessary to protect the cultural and environmental heritage;
- monitor the acquisition phases of cultural property, including the verification of its provenance (e.g. acquiring useful and necessary certifications and authorisations from the seller/supplier).