ANTI-FRAUD CODE

CONTENTS

INTRODUCTION

Intelligence, creativity as well as strategic planning and risk management abilities are some of the attributes positively associated with human beings. However, these same variables may result tremendously harmful when possessed by individuals whose intention is to benefit from them in an inappropriate manner, individuals motivated by the interest of committing fraud.

Today, corporate crises derived from materialization of fraud events are a reality. Fraud has become a possible fact in corporate life, surpassing the classic scenario of cash theft and transcending to new modalities such as deception, breach of trust, willful misconduct and simulation. It may be intentional with forms such as manipulation, forging or alteration of records and documents, embezzlement of assets, deletion or omission of effects of certain transactions in records and documents, recording of unsupported transactions and/or the incorrect application of accounting policies, all of which are enhanced by the easiness and vulnerability of new technological tools.

Accordingly, top management must train the organization to anticipate this type of events and be prepared to deal with them correctly, safeguarding for its stakeholders (shareholders, associates, suppliers, customers, society and the State) every type of asset, especially the financial resources and the information and corporate image.

Thus, from its Corporate Reference Framework, ISA and its companies:

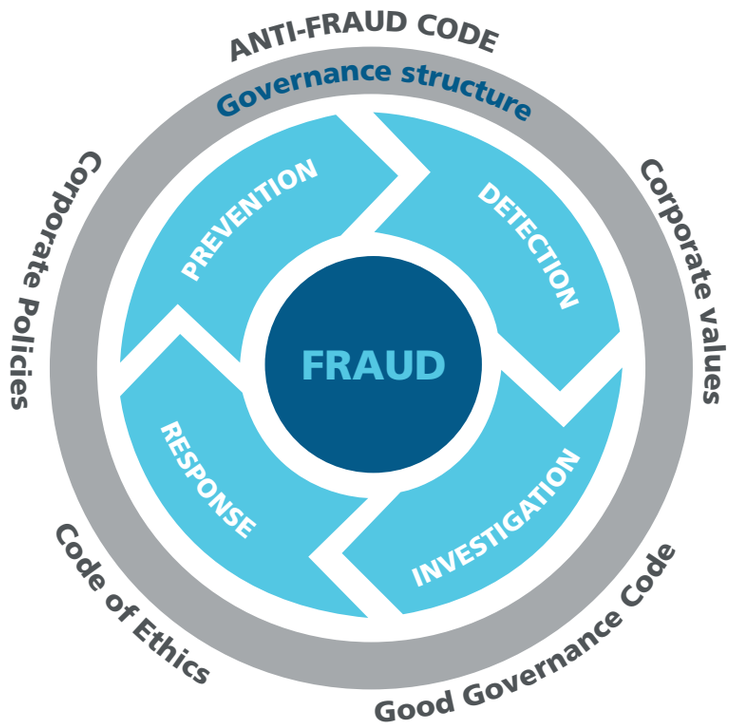
- Establish relations founded on values, policies and commitments that strengthen their corporate identity and institutional coherence;
- Promote management under an ethical and self-control atmosphere;
- Establish the limits that guide corporate actions; and
- Develop processes that guarantee risk management.

Additionally, they incorporate good corporate practices in areas such as prevention and management of fraudulent acts.

MENU

GOAL

The Anti-fraud Code of ISA and its companies is a reference framework intended to formalize their strategic will towards fraud, declaring a no-tolerance culture and establishing corporate guidelines and responsibilities for its prevention, detection, investigation and response.



MENU

CORPORATE REFERENCE FRAMEWORK

Interpretation and application of this Code shall be coherent with the definitions included in the Corporate Framework of ISA and its companies, with special attention to the following related issues:

CORPORATE VALUES

Corporate values identify their will to be and to do, and they bolster their trust and credibility, their form of behavior, and the way they want to achieve recognition.

Values defined are: Ethics, social responsibility, excellence and innovation.

GOOD GOVERNANCE CODE

In this document ISA defines a series of practices regarding its governance, conduct, and handling of information, so that the actions of the shareholders, managers, directive staff and workers are geared to guaranteeing integral corporate ethics, adequate handling of its affairs, respect for those who invest in it, deliverance on the commitments to its stakeholders, and public disclosure of its endeavors.

CODE OF ETHICS

It provides a reference frame that seeks to materialize the philosophy and corporate values of the organization through guiding criteria for the actions of all workers and members of their boards of directors in which every type of fraud is explicitly rejected.

CORPORATE POLICIES

They define and establish action frames that guide the administration of goods and services at all levels of the organization in issues such as internal control, communications, information and knowledge, procurement of goods and services, environment, service, human management, investment, occupational health, social action and integral risk management.

MENU

CONCEPTUAL FRAMEWORK

ISA and its companies define fraud as any intentional action, attempted action, or omission aiming to attain undue benefit in detriment of the corporation's principles and interests. Fraud includes four main categories:

UNDUE APPROPRIATION OR USE OF FINANCIAL RESOURCES AND OTHER ASSETS OF THE COMPANY

Illegal change of destination or undue use of financial resources and other assets of the company and/or managed by it in order to favor own interests or those of third parties. Below is a list of some cases in this category that does not limit the existence of additional ones:

- Undue appropriation or use of assets, equipment or inventories, embezzlement of funds, payments to fictitious suppliers, double payments, manipulation of treasury surpluses, appropriation of moneys and inadequate use of petty cash, among others, owned by the company or administered by it.
- Fictitious compensations.
- Exceeding expenses limits authorized.

INADEQUATE HANDLING OF INFORMATION ASSETS

Creation, access, deletion, modification, alteration, disclosure or use of information assets in an undue and/or fraudulent manner with undue purposes or for personal benefit. Below is a list of information assets included in this category without limiting the existence of additional ones:

- Digital information assets: Structured and non-structured information residing at or transmitted through IT elements and to which the organization assigns a value which must be protected.
- Information assets in other physical and/or electronic media (video, microfilm, etc.): Structured and non-structured information residing at media other than digital media and to which the organization directly assigns a value which must be protected.
- IT elements: Products that support the management of information digital assets. This includes but is not limited to: Workstations, operating systems, mobile devices, printers, software, storage media, servers, user accounts, Internet surfing, networks, electronic mail, file transfer services, among others.

MENU

CORRUPTION

Abuse of power or trust positions for particular benefit. Below is a list of cases included in this category without limiting the existence of additional ones:

- Offering, soliciting, delivering or receiving, goods in kind or in money, in services or in benefits, in exchange for actions, decisions or omissions.
- Accepting gifts for the employee or his family members whose type and amount have been expressly forbidden in the Code of Ethics or in any other institutional document.

FALSEHOOD IN REPORTS

Creation, deletion, modification, alteration or disclosure of any type of information with the aim of distorting the reality of own performance, or that of the company in general or of third parties. Includes the suppression of material information that affects decision-making. Below is a list of cases included in this category without limiting the existence of additional ones:

- Supply of false information to cover deficient performance or to get access to bonuses.
- Use of false reports to deceive investors, financial institutions, regulators or third parties in general.
- Manipulation of financial statements: inappropriate recognition of revenues, over- or sub-estimation of assets, sub-estimation of liabilities, significant estimates not in accordance with the reality of the business, among others.
- Hiding and deliberate violation of exchange, tax, accounting, industrial safety, occupational health, environmental, and energy market regulations, and in general, of regulations applicable to ISA and its companies.
- Hiding of accounting errors.

Fraud may involve dishonest facts from customers, suppliers, representatives, competitors, associates, former associates, managers, directive staff or third parties in general; fraud, therefore, may be put into context of the sources that originate it:

- Internal fraud: Fraudulent actions conducted inside the companies by their workers, directive staff, managers or representatives.

MENU

- External fraud: Fraudulent actions conducted by persons outside ISA and its companies such as suppliers, contractors, customers and third parties in general.

- Mixed fraud: Fraudulent actions conducted with the assistance or participation of internal actors or external persons; those in which one of such actors has the complacence or complicity (by act or omission) of another element of the chain with the purpose of committing a fraud.

MENU

ACTION FRAMEWORK

For ISA and its companies, ethics, as value of values, is an element that differentiates and brings dynamics to its business causing management practices to be conducted under the highest standards of transparency and good corporate practices, incorporating a culture of prevention and administration of fraudulent actions.

Accordingly, ISA and its companies establish the following general criteria that define their will of action with regard to prevention, detection, investigation and response to possible fraudulent actions. Such criteria are mandatory and their interpretation and application are non-discretionary:

1. Promotion of a culture of zero tolerance to fraud. Through their actions and decisions, managers, directive staff and associates set the path of the unconditioned commitment of ISA and its companies to an intolerant position as regards fraudulent actions.

2. The organizational focus adopted is mainly preventive so that vulnerabilities are minimized from the source via adequate criteria for organizational design and cultural transformation programs.

3. Exposure to fraud risk is systematically and periodically evaluated in order to implement effective administration measures that permit both the correct and timely detection and the management of fraud.

4. As to trust relations established with the different stakeholders, ISA and its companies generate an environment of mutual collaboration and respect of common interests; accordingly, they develop anti-fraud strategies that contribute to the strengthening of long-term relations and achievement of corporate sustainability.

5. Managers, directive staff and associates, without exception, shall report to their immediate superior, to the ethics lines, to the auditor's office or to the Ethics Committee, any type of information, doubt or suspicion regarding fraudulent actions. This type of reports shall be handled with absolute reserve and guaranteed confidentiality.

6. Every possible fraudulent action, regardless of its amount, characteristics or implied persons, shall have an answer from the management, who shall verify the facts reported and shall take the relevant administrative actions in abidance by applicable regulation.

7. Companies, when pertinent, shall report to competent authorities every conduct that contradicts this Code and shall bring and support any necessary legal proceedings.

8. In case of fraud, any information required by a stakeholder shall be transparent, impartial and objective, as provided in the Information and Knowledge Policy, in the Communication Policy and, particularly, in the principles defined in the Communication Handbook for Mitigation of Reputational Risks and Crises.

MENU

GOVERNANCE STRUCTURE

Specific responsibilities of the different actors for application of this anti-fraud protocol are defined below:

BOARD OF DIRECTORS

Among the responsibilities related to the adoption of specific measures regarding the Corporation's Governance, the Board of Directors is in charge of:

- Approving this anti-fraud protocol and its updates.
- Providing to the directive staff the material and human elements that permit managing fraud risk.
- Providing guidelines for administration measures and controls that must be established for adequately managing fraud.

AUDIT COMMITTEE

As a supplement to the definitions included in the Board of Directors Decisions, the Audit Committee shall have the following duties:

- Verifying that fraud risk evaluation is correctly made and in accordance with the characteristics of the business, and that effective measures for prevention, investigation and response are implemented.
- Supervising the action plans aimed at minimizing the vulnerabilities of the companies to fraud.
- Providing guidelines regarding controls to be defined for an adequate management of fraud risk.
- Supervising compliance with this protocol.
- Informing to the Board of Directors the fraudulent facts considered relevant.

ETHICS COMMITTEE

In addition to the general responsibilities defined at the Ethics Committees of ISA and its companies, it shall have the following duties:

- Including among plans and programs developed around ethics, activities that foster a culture of fraud prevention.

MENU

- Forwarding to the Audit office or its substitute, the reports made known to it related to possible fraudulent facts.

CHIEF EXECUTIVE OFFICER

In addition to the definitions of internal rulings, the Chief Executive Officer shall have the following duties:

- Promoting implementation of adequate mechanisms for prevention, detection, investigation and response to fraud.
- Making pertinent decisions regarding administrative and judicial actions necessary and always in abidance by applicable regulations.
- Applying the provisions included in the Information and Knowledge Policy, in the Communication Policy and, particularly, in the principles defined in the Communication Handbook for Mitigation of Reputational Risks and Crises, especially with regards to the communication required by stakeholders regarding this Code.

AUDITING

In addition to what has been defined in the internal rulings, the Auditor shall have the following duties:

- Conducting the necessary investigations to clarify possible fraud events independently and in a proficient way and always in compliance with regulations in force, for which purpose he shall adopt a corresponding protocol.
- Ordering the hiring of experts when deemed necessary.
- Planning and evaluating the design and effectiveness of anti-fraud controls.
- Actively participating in the integral management of fraud risk and issuing recommendations regarding the most appropriate strategies to mitigate them.
- Informing the Audit Committee about the internal control evaluations, audits, investigations and related activities.

ASSOCIATES

As defined in the Policy for Integral Management of Risk and in the Internal Control Policy:

- Every associate is responsible for the correct application of the Integral Management of Risk through identification, assessment, handling, monitoring, communication and disclosure of risks associated to their processes and for implementing verification mechanisms.

MENU

- Every associate of the companies of Grupo ISA applies the criteria defined in the Internal Control Policy to build, maintain and exercise effective and efficient controls in the processes and activities under their charge.

- Additionally, and in accordance with this Code, every associate shall report any doubt or suspicion of possible fraudulent facts and cooperate with corresponding investigations.

MENU

MECHANISMS FOR PREVENTION, DETECTION, INVESTIGATION AND RESPONSE

Evaluation of risk exposure is fundamental to its effective management. Such analysis helps to:

- Understand specific possible fraud risks to which the company is exposed;
- Identify possible administration deficiencies; and
- Establish and implement effective mechanisms for its prevention, detection, investigation and response.

Such evaluation shall be made systematically and periodically at both the strategic and operating level.

The evaluation of fraud risk shall be framed within the Policy for Integral Management of Risk and include as a minimum: the evaluation of scenarios or fraud schemes relevant for the company, and their probability and severity, determining the existing mechanisms for prevention, detection and protection. Such evaluation shall establish additional treatment plans necessary to minimize individual vulnerability of the companies. It shall be conducted by those responsible of the process together with the support of the risks and audit team or their substitutes.

Minimum mechanisms for prevention, detection, investigation and response that each company shall implement according to the criteria exposed in this Code:

PREVENTION

The purpose of prevention mechanisms is to minimize the probability of occurrence of fraud thus limiting exposure to them.

It is important to adopt a coherent and integrated approach that takes into consideration all the elements defined in the Corporate Reference Framework, as well as in the institutional guides, procedures and internal rules, so that each of them operates effectively.

In this way, a solid strategy for fraud risk prevention is adopted aiming to incorporate it on a day-to-day basis.

MENU

HUMAN TALENT MANAGEMENT PRACTICES

Given the pivotal role of the human factor in risk prevention, and particularly in fraud risk prevention, it is necessary for each company to evaluate existing mechanisms related to human talent management and to establish their sufficiency and pertinence for such purpose.

SELF-CONTROL PROGRAMS

Self-control is fundamental for fraud risk management; accordingly, every associate shall conduct effectively and efficiently the activities and processes of their daily tasks.

HIRING PRACTICES

As established in the Goods and Services Procurement Policy, transparency is a fundamental criterion defined as follows: "Acquisition processes shall be conducted on the basis of clear, impartial and objective procedures that guarantee equality of conditions and opportunities for all proponents".

With respect to specific fraud risk management, it is necessary for each company to evaluate existing mechanisms for acquisition of goods and services to take into account fraud risk, to determine its sufficiency and relevance and to establish additional elements, if needed.

Additionally, existing procedures shall be adjusted in each company so that this Code becomes mandatory when acting both as contractor and as contracting party.

ETHICS LINE

In line with their preventive focus, ISA and its companies have available an Ethics Line to which associates and stakeholders may communicate their doubts or advising needs in relation to compliance with the Code of Ethics, as well as regarding information that contradicts the provisions of this Anti-fraud Code. Inquiries shall be received guaranteeing the confidentiality of the information and of the person presenting them.

AUDITS

As prevention mechanism, periodic audits at ISA and its companies are a fundamental element of the internal control system that help create an adequate control environment.

Audits conducted shall contribute to the preventive identification of issues requiring improvement in fraud risk management.

SECURITY OF INFORMATION

At ISA and its companies, information, knowledge and products are valued and protected as strategic assets.

Based on the above, principles, models, institutional guides and procedures aimed at guaranteeing information and systems security are provided.

Regarding information security the following corporate guides stand out: Guide for IT Use and Management, Guide for Intellectual Property Protection, Guide for Copyrights and Industrial Property, Guide for Disclosure of Public Information Produced by ISA and its Companies, and the Guide for Documentary Structure.

Additionally, ISA and its companies promote continuous and systematic implementation of best practices for information security and technological controls, including from their structuring, fraud risk management.

DETECTION

As defined in this Code's action framework, effective mechanisms shall be implemented that permit timely detection of possible fraudulent facts so as to minimize their impact. These measures shall be supplemented with the preventive focus defined both at corporate level and for each process. Some of these mechanisms are:

MENU

CONTINUOUS MONITORING

Internal control schemes established for processes shall permit identification of deviations in them in order to have early warnings of possible occurrence of facts contrary to the provisions of this Code.

INTERNAL AUDIT

Audit and follow-up systems reasonably designed in order to detect fraud and irregular conducts are important tools used to determine whether controls at ISA and its companies are operating correctly.

ETHICS LINE

The Ethics Line is conceived as the main medium to communicate fraud suspicious facts. The report shall be received guaranteeing the confidentiality of the information and of the person presenting it.

USE OF TECHNOLOGY

ISA and its companies have provided the technology necessary to support the business' processes and to facilitate natural information flow among processes and among companies, in a technological security environment with confidentiality, reliability and availability criteria.

In addition to traditional detection controls, the company reserves itself the right to monitor its technological environment in order to avoid and detect possible technological frauds respecting confidentiality of information within the framework of applicable law.

Additionally, the aim is effective implementation of early warnings for processes and schemes of continuous monitoring.

INVESTIGATION

Investigation mechanisms include necessary actions to clarify possible fraudulent facts.

When in possession of information regarding fraudulent conducts, ISA and its companies shall carry out any necessary verification in an objective and exhaustive way. The goal of such verifications is to collect relevant information so that the company's management can decide the course of action to follow.

Investigation shall be conducted by the Audit office, or its delegate, using a protocol and respecting regulation applicable in the corresponding country.

RESPONSE

Response mechanisms are aimed at taking corrective measures and repair, if possible, the damage caused by the fraud.

Consequently with the criteria established in this Code's frame of action, fraudulent facts, duly supported and analyzed by the Chief Executive Officer and whoever he considers relevant, will have an administrative and legal response in accordance with applicable internal and external rulings.

Other additional elements to consider are:

INCIDENT HANDLING

In the event of a fraud, its causes and any control weaknesses detected shall be studied and a response plan shall be presented guaranteeing

MENU

that the risk has been managed and that controls will be strengthened. The incident will generate learning to avoid recurrence; issues to take into account are: process redesign, improvement plans, updating of risk evaluation, determination of necessary profile modification and controls adjustment.

TRANSFER

In order to minimize impact of losses and damages caused, ISA and its companies will keep in force risk transfer mechanisms considered relevant according to the evaluation made for risks that so permit.

MENU

APPLICATION AND FOLLOW UP SCOPE

This Code shall be applied to the members of the boards of directors and directories, as well as to every associate regardless of their hierarchical level in the companies.

Compliance with this manual shall be supervised by the Audit Committee or its delegate in each of the companies.

MENU