ITALCER GROUP

DESIGN SURFACES

ORGANIZATION, MANAGEMENT AND CONTROL MODEL AS PER ITALIAN DECREE 231/2001

Summary of the MOGC of Italcer S.p.A. SB
Its implementation and functioning

Updated as at 31.03.2025

ELIOS ceramica · CERAMICA Rondine · BOTTEGA · LA FABBRICA AVA EXTRAORDINARY TILES · AVASTONE · SPRAY DRY

Premise

On 14 December 2021, the Board of Directors of Italcer S.p.A. SB ("Italcer" or the "Company") approved the adoption of the Organization, Management, and Control Model (hereinafter also referred to as the "Organizational Model" or "MOGC") pursuant to Italian Legislative Decree 231/2001.
At the same meeting, the Supervisory Body (hereinafter also referred to as "OdV") was appointed in a collegial composition, whose activities are regulated by the Supervisory Body Regulation. Annually, the OdV drafts and presents to the Board of Directors a report on the activities carried out and an audit plan for the following year.

This document, published on the Company's website, aims to illustrate the guidelines that inspired the adoption and implementation of the Organizational Model itself, through an in-depth analysis of the related application steps.

The CEO
Dr. Graziano Verdi

Index

1
Mechanisms of operation of Legislative Decree 231/2001

Legislative Decree 231/2001 extends to entities the consequences of criminally relevant conducts carried out by individuals operating within it as administrators, employees, or consultants. The involvement of the company occurs when four conditions **simultaneously combine**:

Italcer is an **entity subject** to the provisions of Legislative Decree 231/2001.

It is necessary to analyze the organizational chart to identify the individual person:

- with legal representation (top managers)
- with formal delegation of powers (top managers)
- who perform management functions (top management)
- who exercise management and control power (top management)
- who are subject to direction and supervision (subordinate)

The offenses that can involve the entity are exclusively those included in the catalog of the Decree

The entity is liable if the person who committed the offense acted in the entity's own exclusive **interest** or **advantage**.
The entity is not liable if the person who committed the offense **acted in their own exclusive interest or that of third parties.**

1.1 The catalog of offenses

The sanctions provided by Legislative Decree 231/2001 apply to a wide range of offenses.

Below are the categories of offenses that, with varying levels of risk, can constitute sensitive areas of application of the Decree in respect of our Company:

1. Manslaughter or serious or very serious injuries committed in violation of **health** and safety regulations at work
2. **Environmental** Crimes
3. **Cyber** Security Crimes
4. Crimes against **Public Administration**
5. **Corporate and Tax** Crimes

1.2 The presumed involvement of the entity

Legislative Decree 231/2001 establishes a sort of **automatism**. When a top manager or subordinate commits one of the offenses provided for by the decree in the **interest** or **advantage** of the entity for which they work, THE ENTITY IS ALWAYS RESPONSIBLE, unless it has implemented appropriate prevention and control measures.

WHICH?

- demonstrate that the appropriate countermeasures have been implemented to **prevent and control** the conduct of the person who committed the offense
- demonstrate that the person who may have committed the offense did so by **fraudulently violating** the prevention and control system

The system of countermeasures and/or safeguards is called the **ORGANIZATIONAL MODEL** (or organizational management and control model, known as **MOGC**). If an entity can demonstrate the existence of countermeasures and/or safeguards, it means that it has a MOGC, which is a set of rules and procedures aimed at preventing and controlling the commission of offenses provided for in the decree by its top managers or subordinates. In the event of a fatal incident (charge against a top manager), the existence of the model, even before demonstrating its efficiency, **PROTECTS AGAINST PRECAUTIONARY MEASURES THAT COULD BE TAKEN AGAINST THE ENTITY (ARTS. 49 and 17 of Legislative Decree 231/2001)**.

1.3 The prevention and control function of the Organizational Model

PREVENTION:

Continuous training

Code of ethics

Disciplinary code

Policies and procedures

OdV

LOW COMPLEXITY ACTIVITY

CONTROL:

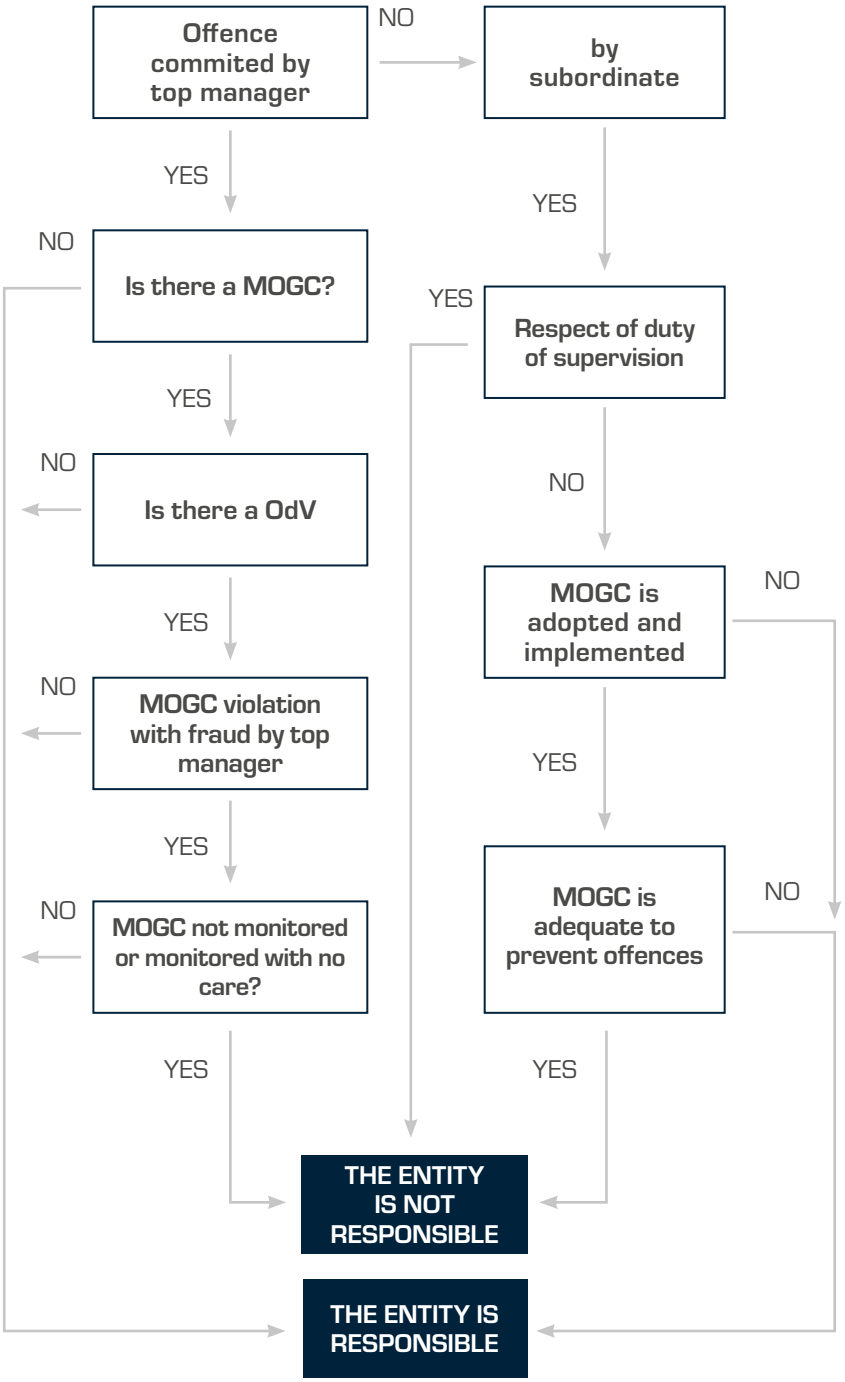
Control Periodic information flow to the OdV and the Internal Audit on the state of efficiency and functioning of the Organizational Model

Periodic information flow to the OdV and the Internal Audit on the updated of the MOGC consequent to regulatory changes

HIGH COMPLEXITY ACTIVITY

1.4 The exonerating function of the Organizational Model

In case of a negative event, the Organizational Model must be able to exercise the exonerating function before the investigating authority.



In case of an offence commited by a **Top Manager**, the MOGC is necessary because the ENTITY, to be exempted, **MUST PROVE** (burden of proof reversal) that:

1. To have implmented prevention tool such as:
   - MOGC **adoption**;
   - MOGC **implementation**;
   - MOGC functioning **supervision**;
2. that the top manager who committed the offense did so by **fraudulently circumventing** the MOGC;
3. that the **Supervisory Body (ODV)** has monitored the MOGC without omissions or negligence

In case of an offense committed by a **subordinate**, the MOGC is necessary because the ENTITY, to be exempted, MUST prevent the judge from **PROVING that:**

1. the commission of the offense took place **because of lack** of **direction** and **supervision** by the top managers, over the activity of the subordinate
2. there is an organizational model that provides for the direction and supervision by the top managers over the subordinates, but the said model **does not meet the criteria of efficiency** or that the mechanisms of direction and supervision have not work properly.

2
Implementation of the MOGC

PRELIMINARY CONTEXT ANALYSIS

- Analysis of the activity carried out
- Passive cycle
- Active cycle
- Production cycle with physical and legal description of the production layout
- Analysis of the social and industrial context in which the Company operates
- Information about employees
- Information about technological infrastructure
- Information about the structure of internal and external controls

RISK ASSESSMENT

- Identification of potential 231 risk areas
- Assessment of inherent risk and residual risk for each individual area
- Classification of areas based on the degree of risk
- Measurement of the GAP between current compliance and theoretical 100% compliance

REMEDIATION PLAN

It derives from the Risk Assessment and is carried out annually, highlighting the remediation actions based on the urgency with which they must be implemented. It provides a control tool on the progress of compliance work.

CODE OF ETHICS

Italcer Group has adopted a Code of Ethics that represents the fundamental tool for safeguarding and transmitting the most authentic values and principles that are the true pillars of the Group's entrepreneurial philosophy. Specifically, the Code of Ethics represents the set of positive principles and rules of conduct that the Group's companies have voluntarily chosen to adopt and make public, as a concrete expression of their intentions towards stakeholders.

DISCIPLINARY CODE

The disciplinary code, within the Organizational Model, plays a fundamental role in ensuring compliance and adherence to the Organizational Model itself. Its main objectives are designed to preserve integrity, legality, and the correct application of company rules and regulations.

CONTINUOUS TRAINING

Continuous training has been implemented since the day of the adoption of the MOGC and is mainly carried out in the classroom with learning assessment systems.

General part

Contains the fundamental principles of the risk management system, including the regulatory framework, the objectives of the MOGC, the code of ethics, the disciplinary system, and the tasks of the Supervisory Body.

1. Company profile
2. Mechanisms of operation of Legislative Decree 231/2001
3. The Audit, Risk, and Compliance (ARC) functions for the MOGC
4. Implementation of the organizational model 231
5. The digitization of the dynamic organizational model

Special part

It goes into detail about the individual categories of predicate offenses provided for by Legislative Decree 231/2001, identifying risk areas and specific prevention measures adopted by the Company for each type of offense.

Its components are:

1. Company information preparatory to the adoption and implementation of the Organizational Model pursuant to Legislative Decree 231
2. Risk assessment
3. Existing prevention tools (code of ethics and disciplinary code, training plan)
4. Reporting tools
5. Methods of managing sensitive data
6. Remediation plan

The management of Italcer's MOGC relies on a repository of documents and related processes aimed at preventing and controlling the commission of 231 offenses. The repository is based on an interactive organizational chart and a sociogram that allow each employee to be linked to the processes he/she manage or is involved in, tracing the history.

2.1 Risk Assessment

2.1.1 Definitions

Inherent risk represents the level of exposure of an organization to a potentially harmful event, calculated before the application of any control or mitigation measures. It is a 'pure' risk and intrinsic to the process, activity, or operational environment in which the organization operates.

Residual risk, on the other hand, represents the level of risk that 'remains' after the implementation, even partial, of control, mitigation, and prevention measures. Before implementing these measures, it is the risk that the organization continues to face, despite the existence of procedures and management systems. In other words, in the absence of countermeasures, residual risk corresponds to inherent risk.

Probability represents the estimated frequency or likelihood that a risky event will occur in a given context and depends on various intrinsic and extrinsic factors related to the activity or process analyzed.

Impact, on the other hand, represents the severity of the consequences that a risky event can cause. It reflects the level of potential damage or loss in economic, regulatory, operational, reputational, or environmental terms.

2.1.2 Methodology

1. Identification of potential **risk areas** applicable to the entity
2. Assessment of **inherent risk** and **residual risk** for each individual area
3. **Classification** of areas based on the degree of risk
4. Measurement of the **"GAP"** between contexts with real residual risk and contexts with zero theoretical residual risk
5. Identification of **remedial and/or risk mitigation actions**
6. Definition of a **remediation plan** for the execution of identified actions

2.1.3 Use of artificial intelligence

The use of AI allows synthesizing the first 5 activities mentioned above into a single process through sequential algorithms, based on the following steps:

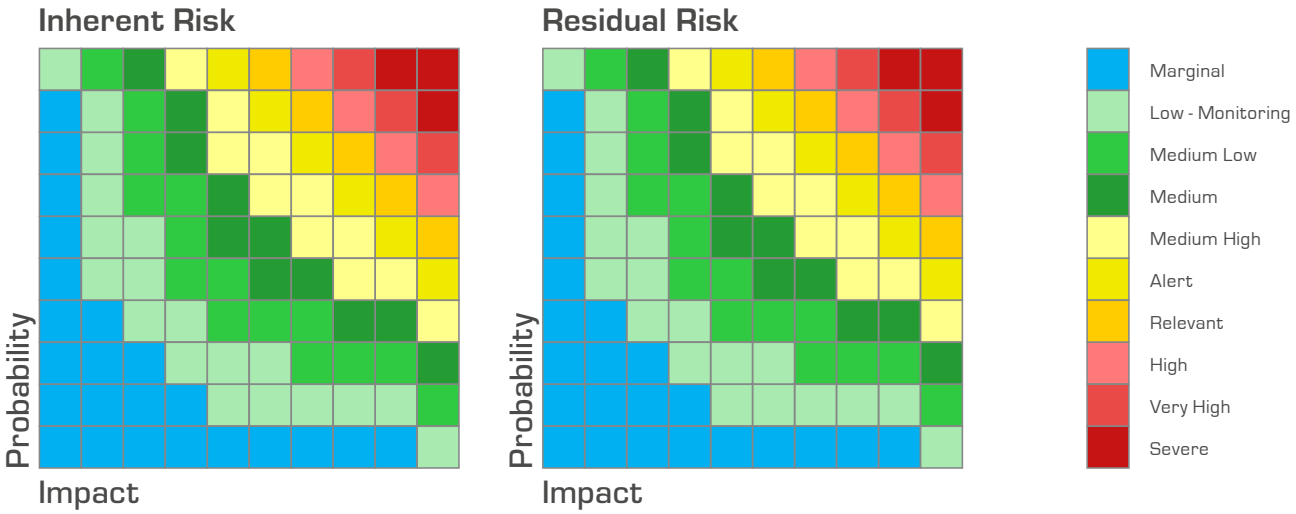
1. Creation of personalized checklists
2. Completion of checklists
3. Creation of the algorithm to obtain responses for each category of offense in terms of assessment of inherent risk and residual risk based on the probability of occurrence and potential impact
4. Generation of inherent and residual risk assessments
5. Generation of remedial actions.

The algorithm processes data on four levels:

- **Level 1:** on the type of offense and its conduct
- **Level 2:** on contexts of the type of offense identified by the algorithm (from 1 to N contexts)
- **Level 3:** for each context, measurement of probability and impact of the event with reference to inherent risk (from 1 to 10 degrees)
- **Level 4:** for each context, measurement of probability and impact with reference to residual risk (from 1 to 10 degrees).

LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
OFFENCE	CONTEXT	INHERENT RISK	RESIDUAL RISK
	Context 1	Probability (from 1 to 10)	Probability (from 1 to 10)
		Impact (from 1 to 10)	Impact (from 1 to 10)
	Context 2	Probability (from 1 to 10)	Probability (from 1 to 10)
		Impact (from 1 to 10)	Impact (from 1 to 10)
	Context N	Probability (from 1to10)	Probability (from 1 to 10)
		Impact (from 1 to 10)	Impact (from 1 to 10)

		INHERENT RISK	RESIDUAL RISK
FINAL EVALUATION	1	Marginal	Marginal
	2	Low	Low
	3	Medium Low	Medium Low
	4	Medium Low	Medium Low
	5	Medium High	Medium High
	6	Alert	Alert
	7	Relevant	Relevant
	8	High	High
	9	Very High	Very High
	10	Severe	Severe



2.1.4 Identification of first-level variables

	OFFENCES	OFFENCES RISK AREA	RELEVANCE DEGREE ACCORDING TO THE RISK ASSESSMENT	ACTIONS
1	UNLAWFUL RECEIPT OF DISBURSEMENTS, FRAUD AGAINST THE STATE, FRAUD IN PUBLIC SUPPLIES, AND COMPUTER FRAUD (ART. 24)	Against the state (24)	Potential risk – necessary risk assessment	Risk assessment
2	CIBER CRIMES AND UNLAWFUL DATA PROCESSING (ART. 24-BIS) (ART. 24-BIS)	Cyber - 24bis	Potential risk – necessary risk assessment	Risk assessment
3	ORGANIZED CRIME OFFENSES (ART. 24-TER)	Organized crime (24ter)	Conduct not applicable with no real risk	NONE
4	EMBEZZLEMENT, EXTORTION, UNDUE INDUCEMENT, CORRUPTION, AND ABUSE OF OFFICE (ART. 25)	Corruption extortion - 25	Conduct applicable but with zero inherent risk	Monitoring
5	COUNTERFEITING OF CURRENCY, PUBLIC CREDIT CARDS, AND STAMP VALUES (ART. 25-BIS)	Counterfeiting of currency - 25.2	Conduct not applicable – no risk assessment necessary	NONE
6	INDUSTRY AND COMMERCE OFFENSES (ART. 25-BIS.1)	Industry and commerce offenses (25.2.1)	High residual risk – necessary risk assessment	Monitoring
7	CORPORATE CRIMES (ART. 25-TER)	Corporate crimes (25.3)	Potential risk – necessary risk assessment	Risk assessment
8	CRIMES WITH THE PURPOSE OF TERRORISM OR SUBVERSION OF THE DEMOCRATIC ORDER (ART. 25-QUATER)	Terrorism (25.4)	Conduct not applicable – no risk assessment necessary	NONE
9	PRACTICES OF FEMALE GENITAL MUTILATION (ART. 25-QUATER.1)	Mutilation (25.4.1)	Conduct not applicable – no risk assessment necessary	NONE
10	CRIMES AGAINST INDIVIDUAL PERSONALITY (ART. 25-QUINQUIES)	Indivisual personality (25.5)	Conduct not applicable – no risk assessment necessary	NONE
11	MARKET ABUSE OFFENSES (ART. 25-SEXIES)	Market abuse (25.6)	Conduct not applicable – no risk assessment necessary	NONE
12	MANSLAUGHTER AND NEGLIGENT PERSONAL INJURIES IN VIOLATION OF WORKPLACE SAFETY REGULATIONS (ART. 25-SEPTIES)	Workplace safety (25.7)	Sensitive inherent risk – necessary risk assessment	NONE
13	RECEIVING, LAUNDERING, USING MONEY, GOODS, OR BENEFITS OF ILLICIT ORIGIN, AND SELF-LAUNDERING (ART. 25-OCTIES)	Money laundering and self-laundering (25.8)	Zero inherent risk even if potential - necessary monitoring	Monitoring

	OFFENCES	OFFENCES RISK AREA	RELEVANCE DEGREE ACCORDING TO THE RISK ASSESSMENT	ACTIONS
14	PAYMENT INSTRUMENTS OTHER THAN CASH (ART. 25-OCTIES.1)	Payment instrument (25.8.1)	Conduct not applicable – no risk assessment necessary	NONE
15	COPYRIGHT INFRINGEMENT (ART. 25-NOVIES)	Copyright (25.9)	Zero inherent risk even if potential - necessary monitoring	Monitoring
16	INDUCEMENT NOT TO MAKE STATEMENTS TO THE JUDICIAL AUTHORITY (ART. 25-DECIES)	False statements (25.10)	Conduct applicable but with zero risk	NONE
17	ENVIRONMENTAL CRIMES (ART. 25-UNDECIES)	Environmental savety (25.11)	High inherent risk – necessary risk assessment	Risk assessment
18	EMPLOYMENT OF THIRD-COUNTRY NATIONALS WHOSE STAY IS IRREGULAR (ART. 25-DUODECIES)	Irregular employment (25.12)	Potential risk but zero in practice - no risk assessment necessary	NONE
19	RACISM AND XENOPHOBIA (ART. 25-TERDECIES)	Racism (25.13)	Potential risk but zero in practice - no risk assessment necessary	NONE
20	FRAUD IN SPORTS COMPETITIONS (ART. 25-QUATERDECIES)	Sport fraud (25.14)	Conduct not applicable – no risk assessment necessary	NONE
21	TAX CRIMES (ART. 25-QUINQUIESDECIES)	Tax crimes (25.15)	Potential risk – necessary risk assessment	Risk assessment
22	SMUGGLING (ART. 25-SEXIESDECIES)	Smuggling (25.16)	Conduct not applicable – no risk assessment necessary	NONE
23	TRANSNATIONAL CRIMES (ART. 10 DELLA L. 146/2006)	Transnational crimes	Conduct applicable but with zero risk	NONE
24	CYBER SECURITY OF CRITICAL INFRASTRUCTURES	Cyber security	Included in the risk assessment of cyber crimes	Included in the risk assessment

2.1.5 Identification of second-level variables

WORKPLACE SAFETY AREA

- Use of checklists based on the prescriptions of Legislative Decree 81 of 2008
- Mapping of INAIL prescriptions and guidelines
- Integration with obtained ISO certifications (ISO 9001, ISO 14001, ISO 450001, ISO 50001)

ENVIRONMENTAL SAFETY AREA

- Use of checklists based on company data such as (i) number of plants, (ii) average size of plants, (iii) degree of production automation, (iv) production shifts, (v) average age of plants, (vi) involved personnel, etc.
- Evaluation of the riskiness of each plant based on the national ARPA classification in relation to (i) soil pollution, (ii) subsoil pollution, (iii) water pollution, (iv) air pollution, and (v) waste disposal.

CYBER SECURITY AREA

- Evaluation of the occurrence of incident threats foreseen by the European authority for cyber piracy control (ENISA), namely: (i) ransomware, (ii) malware, (iii) cryptojacking, (iv) email attacks, (v) data attacks, (vi) web attacks, (vii) disinformation, and (viii) misinformation.

CORPORATE CRIMES AREA

- Evaluation based on checklists that take into account (i) company context; (ii) internal control systems (such as internal audit procedures and protocols, CFO, and IT function) and external control systems (audit firms, board of statutory auditors, and Supervisory Body).

TAX CRIMES AREA

- Evaluation based on checklists that take into account: (i) company context; (ii) interaction with foreign entities (mainly customers) located in all territories of the world; (ii) criticality of international transactions; (iv) supplier selection procedures and KYC on customers.

CRIMES AGAINST THE STATE AREA

- Evaluation based on checklists drawn up with reference to the guidelines of ENAC (National Anti-Corruption Authority), taking into account (i) company context; (ii) active and passive cycle and absence of interaction with public entities; (iii) perception of public funding and contributions.

2.2 The Remediation Plan – an excerpt

TASK REMEDIATION PLAN		MONTH 2025								
Workplace safety (art. 25 - septies)	**Task manager**	4	5	6	7	8	9	10	11	12
Mitigation/remediation action										
Mitigation/remediation action										
Environmental crimes (art. 25 - undecies)	**Task manager**									
Mitigation/remediation action										
Mitigation/remediation action										
Cyber crime (art. 24 - bis)	**Task manager**									
Mitigation/remediation action										
Mitigation/remediation action										
Crimes against the State (art. 24)	**Task manager**									
Mitigation/remediation action										
Mitigation/remediation action										
Corporate crimes (art. 25 - ter)	**Task manager**									
Mitigation/remediation action										
Mitigation/remediation action										

The Internal Audit and the OdV monitor the execution of the remediation plan based on an audit plan shared with the Board of Directors.

The system provides appropriate reports for both the Supervisory Body and the Internal Audit.

3
Maintenance and periodic updating of the MOGC

NEW RISK ASSESSMENT

Risk assessments revision based on the following:

1. Analysis of the **progress of activities** from the previous year's remediation plan
2. **Changes in contextual information** (active cycle, passive cycle, production cycle, diversification, differentiation, opening new markets, etc.)
3. **Regulatory changes** in the laws governing compliance in risk areas

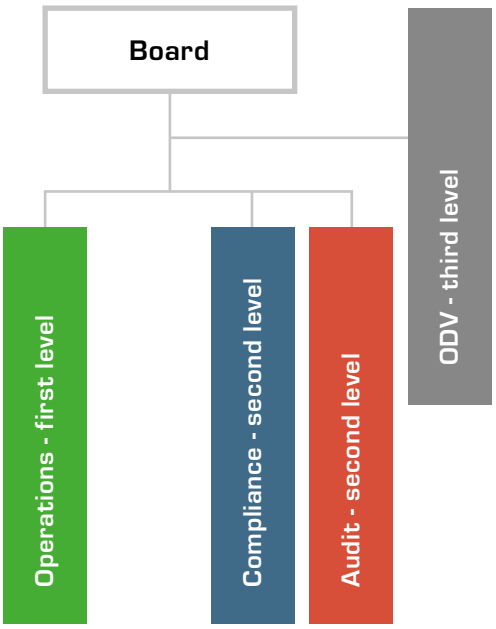
NEW REMEDIATION PLAN

Revision of the **remediation actions** to be implemented because of the risk assessment Changes.

NEW AUDIT PLAN

Revision of the **audit plan** because of the remediation plan Changes

4
The control function



The control function of Italcer is set up on three levels:

first-level control over operations, based on individual operating procedures, performed by managers at various levels of the organizational chart;

second-level control performed by the Compliance & Internal Audit function, identified in a managerial figure, also internal member of the Supervisory Body, with access to the repository;

Third-level control performed by the OdV appointed by the Board of Directors and provided with spending powers.

The Internal Audit can be contacted at the following email address:
audit@gruppoitalcer.it

5
The Supervisory Body

Pursuant to Articles 6, 7, and 8 of Legislative Decree 231 of 2001, the Board of Directors that approved the Organizational Model also appointed a collegial Supervisory Body, composed of 3 members, who have adopted an autonomous regulation and have been provided with an autonomous spending budget.

The current Supervisory Body is composed of the following members:

- Dr. Giovanni Taliento
- Dr. Ilaria Patri
- Lawyer Marika Rossi

The Supervisory Body can be contacted at the following email address:
organismodivigilanza@gruppoitalcer.it

6 Whistleblowing

With Law of November 30, 2017, No. 179 containing the "Provisions for the protection of authors of reports of crimes or irregularities of which they have become aware within the scope of a public or private employment relationship" (hereinafter also referred to as the "Whistleblowing Law"), the Legislator, in an attempt to harmonize the provisions provided for the public sector with the aforementioned Law, introduced specific provisions for entities subject to Legislative Decree No. 231/2001 and inserted three new paragraphs within Article 6 of Legislative Decree No. 231/2001, namely paragraphs 2-bis, 2-ter, and 2-quater.

Our Organizational Model provides that the Recipients, who in the performance of their duties, detect or become aware of possible illegal or irregular behaviors carried out by individuals who have various relationships with the Company, are required to promptly report the facts, events, and circumstances that they believe, in good faith and based on reasonable factual elements, have determined such violations and/or conduct not in compliance with the Company's principles.

Reports must be transmitted through a reserved and managed channel, accessible at the following link: **https://italcer.integrityline.com**

ITALCER GROUP

DESIGN SURFACES

WWW.GRUPPOITALCER.IT