

# **INTERNAL CONTROL SYSTEM AND RISK MANAGEMENT GUIDELINES OF THE COGNE GROUP**

# TABLE OF CONTENTS

<b>PURPOSE</b>	<b>2.</b>
<b>SCOPE OF APPLICATION</b>	<b>2.</b>
<b>RECIPIENTS</b>	<b>2.</b>
<b>BEHAVIORAL RULES</b>	<b>2.</b>
<b>WHAT IS THE INTERNAL CONTROL SYSTEM AND RISK MANAGEMENT?</b>	<b>3.</b>
<b>THE REFERENCE FRAMEWORK OF THE INTERNAL CONTROL SYSTEM AND RISK MANAGEMENT</b>	<b>3.</b>
<b>GOVERNANCE</b>	<b>5.</b>
<b>IMPLEMENTATION OF THE INTERNAL CONTROL SYSTEM</b>	<b>11.</b>
<b>COMMUNICATION AND INFORMATION</b>	<b>13.</b>
<b>MONITORING AND REPORTING</b>	<b>15.</b>
<b>REVIEW OF THE GUIDELINES</b>	<b>16.</b>



## 1. PURPOSE

The Internal Control System and Risk Management Guidelines of the Cogne Group, hereinafter referred to for brevity as ICS or ICSRM, are composed to provide the Recipients with a description of the current system, illustrating its various components.

## 2. SCOPE OF APPLICATION

The contents of these Guidelines apply to Cogne Acciai Speciali S.p.A. and all Companies directly controlled by the Cogne Group, unless otherwise specified by the compliance and/or governance models adopted by those companies in consideration of specific applicable legal and regulatory provisions and/or the characteristics of the individual companies<sup>1</sup>.

## 3. RECIPIENTS

The Guidelines apply to all employees of the Cogne Group, as they are involved, within their respective areas of responsibility and in line with their assigned duties, in maintaining and improving the Internal Control and Risk Management System of Cogne Acciai Speciali S.p.a. and of the directly controlled Companies.

## 4. BEHAVIORAL RULES

All personnel of the Cogne Group (Cogne's People) are required to comply with current laws and regulations, the behavioral standards referenced in the Code of Business Conduct, and the Guidelines contained in this document.

## 5. WHAT IS THE INTERNAL CONTROL SYSTEM AND RISK MANAGEMENT?

The Internal Control System and Risk Management consists of the set of tools, rules, procedures, and corporate organizational structures aimed at effectively and efficiently identifying, measuring, managing, and monitoring the main risks, to contribute to the company's sustainable success. An effective Internal Control and Risk Management System supports the operation of the company in alignment with the business objectives defined by the Board of Directors, fostering informed decision-making. It helps to ensure:

- The protection of company assets,
- The efficiency and effectiveness of business processes,
- The reliability of information provided to corporate bodies and the market,
- Compliance with laws and regulations, as well as with the company's by laws and internal procedures.

## 6. THE REFERENCE FRAMEWORK OF THE INTERNAL CONTROL SYSTEM AND RISK MANAGEMENT

For the definition of its ICSRM, the Cogne Group has drawn inspiration from the standards "Internal Control System", "Enterprise Risk Management – Integrated Framework CoSO ERM Framework" and the Corporate Governance Code, as these represent international and national benchmarks and best practices for the design, development, and evaluation of the ICSRM itself.

This standard serves as an analytical tool capable of assessing the Company's Internal Control System and the risk management model in its various components, providing Management with a clear view of areas for improvement in terms of the effectiveness and efficiency of the Internal Control System.

The ERM Framework supports the proper achievement of business objectives (strategic, operational, reporting, compliance) and is composed of eight interconnected components integrated into processes and all organizational levels, as illustrated in the figure.

Specifically, the eight components of the ERM Framework correspond respectively to:

- **Internal Environment:** constitutes the essential identity of the organization. It determines how risk is perceived and addressed by company personnel, including the risk management philosophy, acceptable levels of risk, integrity, ethical values, and the general work environment.



- **Objective Setting:** objectives must be established before identifying events that may potentially jeopardize their achievement. They should support the company's mission, be consistent with it, and aligned with acceptable levels of risk.
- **Event Identification:** involves the correct and comprehensive identification and classification of all events, both internal and external, that could partially or completely impair the achievement of business objectives and therefore represent potential risks to be managed.
- **Risk Assessment:** introduces an evaluative component capable of quantifying the level of "inherent risk" (risk in the absence of any intervention) and the level of "residual risk" (the remaining risk after considering mitigation measures). Risk levels should be quantified by considering the impact on achieving company objectives and the likelihood of occurrence.

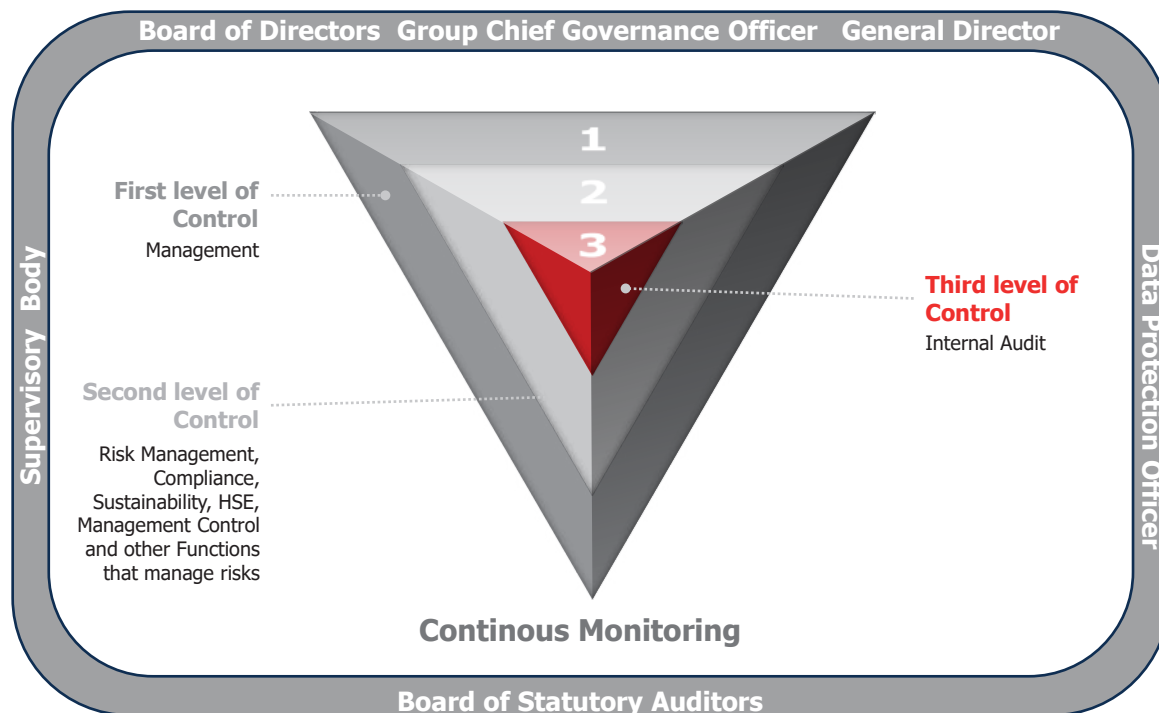
- **Risk Response:** concerns the selection and implementation, by management, of interventions aimed at managing the identified risk, reducing it, and aligning it with the “tolerated” or “accepted” risk levels.
- **Control Activities:** refers to the need to define, implement, and apply appropriate policies and procedures to ensure that risk responses and mitigation measures are effectively executed.
- **Information & Communication:** information must be identified, collected, and disseminated in a timely and appropriate manner to enable all resources involved in the process to operate correctly and efficiently.
- **Monitoring:** refers to the company’s “ability” to self-assess and to continuously update/improve over time.

It is important to note that the ERM Framework, in addition to being applied to financial, operational, or compliance risks, has also been extended to Environmental, Social & Governance (ESG) risks, as the process of identifying, evaluating, and managing ESG risks is itself a relevant strategic objective for every company.

From the perspective of the Cogne Group, in fact, the quality and actual application of risk management aligned with ESG issues is directly proportional to the company’s ability to create stable and long-term economic value.

## 7. GOVERNANCE

The Cogne Group has established, for all directly controlled companies, the position of Group Chief Governance Officer, who is responsible for overseeing Governance, Sustainability, Compliance, the Internal Control System, Risk Management, and Insurance. This role is in charge of developing, implementing, and monitoring governance and management policies to ensure that the Group operates ethically, in full compliance, efficiently, sustainably, and in strategic alignment with the directives defined by Cogne Acciai Speciali S.p.A. and Walsin Lihwa Corporation.



Key players of the Internal Control System at Cogne Acciai Speciali S.p.A. are:

### 7.1 Board of Directors

The Board of Directors (BoD):

- Evaluates the adequacy of the company's overall organizational, administrative, and accounting structure, and, after consulting with the control body, assesses the results presented by the external auditor in any letter of suggestions and in the additional report addressed to the Board of Statutory Auditors.
- Appoints and dismisses the Head of Internal Audit, ensuring they are provided with adequate resources to perform their duties and compensated in line with company policies.
- Approves the audit plan prepared by the Internal Audit Director, after consultation with the control body.
- Approves, upon proposal of the Group Chief Governance Officer, the Cogne Group Guidelines in accordance with the provisions of Walsin Lihwa Corporation.
- Describes, in the corporate governance report, the main characteristics of the ICS and the coordination mechanisms among the involved parties, expressing its assessment on its adequacy.
- Approves the Organization, Management and Control Model pursuant to Legislative Decree 231/2001 ("Model 231") and any related amendments and appoints and dismisses the members of the Supervisory Body provided for by the Decree.
- Approves the Risk Appetite level based on the Risk Management methodology defined.

## 7.2 General Director

The General Director, in addition to holding the powers necessary to carry out all operational acts related to the company's activities:

- Implements appropriate organizational, administrative, and accounting arrangements together with the Chief Executive Officer.
- Carries out the strategic directives defined by the Board of Directors, overseeing the design, implementation, and management of the Internal Control System and constantly verifying its overall adequacy, effectiveness, and efficiency.
- Manages the identification of key company risks, considering the specific features of the company's and its subsidiaries' activities, and periodically submits them for review by the Board of Directors.
- Adapts the system to changes in operational conditions and the legal and regulatory landscape.
- When necessary, requests the Internal Audit Department to perform audits on specific operational areas and on compliance with internal rules and procedures during company operations, simultaneously informing the Chairman of the Board of Directors and the Chairman of the Board of Statutory Auditors.
- Promptly reports to the Board of Directors and the Board of Statutory Auditors on issues and criticalities that arise during the performance of their duties or that come to their attention, so that appropriate actions may be taken.

## 7.3 Board of Statutory Auditors

The Board of Statutory Auditors performs the duties assigned to it by law and by the company's bylaws. Specifically, the Board of Statutory Auditors of Cogne Acciai Speciali S.p.A. monitors:

- Compliance with legal provisions and the bylaws.
- Respect for sound management principles.
- The adequacy of the organizational, administrative, and accounting system adopted by the Company and its proper functioning.

The Board of Statutory Auditors may make use of the Internal Audit Department to conduct audits on specific operational areas or company operations.

## 7.4 Supervisory Board

The Supervisory Body, appointed by the Board of Directors, is responsible for overseeing the functioning and compliance of the Organization, Management and Control Model adopted pursuant to Legislative Decree 231/2001 and ensuring its updates. The roles and responsibilities of the Supervisory Body are defined in the Model itself. The Supervisory Body, which includes the Internal Audit Director, may also rely on the Internal Audit Department to carry out audit and/or verification activities on specific issues.

## 7.5 Data Protection Officer

The Data Protection Officer (DPO) is responsible for advising the Data Controller and employees regarding obligations under the GDPR, and for monitoring compliance with these requirements. The DPO ensures a structured and effective coordination of Data Protection topics through the adoption and use of digital platforms and shared documentation standards.

For a detailed list of the DPO's responsibilities, please refer to current legal and regulatory provisions.

## 7.6 First Level of Control: Management

Management, based on the responsibilities assigned to it within the company's organizational structure, ensures the effective functioning of the ICS as part of its accountability in achieving objectives. At every level of the organization, Management represents the first line of control of the system. Therefore, Management must possess the necessary knowledge, training, and capacity to act and operate within the ICS, and must be empowered to fulfill the tasks associated with their role. This implies that everyone has both the right and the duty to fully understand and be familiar with the Company and the Cogne Group, its operational mechanisms, objectives, markets, and the risks to which it is exposed. Furthermore, all personnel of the Cogne Group, each according to their respective competencies, must contribute to ensuring the effective functioning of the ICS, by reporting issues to the appropriate corporate contacts based on the topic identified.

## 7.7 Second Level of Control: Involved Functions

Second-level control functions are roles with specific responsibilities for monitoring and overseeing different areas/types of risk. These functions monitor business risks, propose guidelines for relevant areas of the Control System, and verify the adequacy of controls to ensure: operational efficiency and effectiveness; adequate risk control; prudent business conduct; reliability of information; and compliance with laws, regulations, and internal procedures.

These functions are independent and separate from operational activities. They contribute to defining risk governance policies and to the process of risk management.

### 7.7.1 ICS, Risk Management and Compliance Department

The ICS, Risk Management and Compliance Department:

- Develops Guidelines for its areas of responsibility concerning the Internal Control and Risk Management System of the Cogne Group in line with Walsin Lihwa Corporation's requirements.
- Defines and acts as facilitator of the common methodology for risk analysis and evaluation, and is responsible for risk assessment activities.
- Ensures the enhancement of the Internal Control and Risk Management System through risk evaluation and the definition of lean, adequate, and effective controls to achieve the best balance between risks, controls, and business performance.
- Promotes and enables a continuous monitoring system to integrate risk management into business operations, supporting strategic decisions and aligning them with corporate objectives, including through the use of artificial intelligence and analytics.
- Defines and oversees the regulatory compliance system, including trade compliance, managing related risk assessment activities in coordination with the relevant business functions.
- Verifies the consistency of internal control measures defined by company regulations with applicable laws.
- Analyzes relevant legislation and ensures the updating of Organization, Management and Control Models under Legislative Decree 231/2001.
- Prepares the second-level audit plan, defines audit execution methods, and carries out such audits.
- Oversees anti-corruption risks and other integrity-related risks through an approach that facilitates synergies among key stakeholders, integration between business and values, results, and rules.
- Evaluates the compliance of new processes in advance.
- Provides advice to support the business.
- Conducts training on its areas of expertise.

- Promotes a culture of integrity at all levels.
- Implements measures to prevent and effectively manage potential fraud, through the design, implementation, and continuous improvement of the anti-fraud model.
- Supervises, also in its capacity as Anti-Corruption Compliance Officer, the implementation and improvement of the Anti-Corruption Management System and ensures its compliance with UNI ISO 37001:2016.
- Monitors business interruption events and related action plans, supporting the business in applying business continuity protocols.
- Conducts second-level audits and continuous monitoring regarding the implementation of business continuity models, ensuring that findings are shared with the relevant business units.
- Ensures the dissemination of shared standards and methodologies, for its areas of responsibility, throughout the Cogne Group companies.
- Supports Management in defining corrective actions following the outcomes of Internal Audit activities and, if necessary, assists in their implementation.

## 7.7.2 Sustainability and Corporate Affairs

The Sustainability and Corporate Affairs Function:

- Supports company management in defining strategies and related business objectives in the field of sustainability.
- Ensures the feasibility of the sustainability strategy by identifying KPIs and performance metrics within business areas.
- Implements the Group's sustainability reporting process in line with the defined strategy;
- Prepares the sustainability report.
- Identifies internal control measures specifically related to sustainability issues and the quality of related data.
- Promotes the definition of guidelines and procedures to implement sustainability policies;
- Identifies the link between the priorities set out in business strategies and their impact on the Sustainable Development Goals of the 2030 Global Agenda, highlighting how the company can contribute to achieving them.
- Analyzes applicable regulations and ensures compliance with them regarding sustainability topics.
- Prepares documentation and reports for senior management and drafts texts related to sustainability matters.
- Ensures the dissemination of shared standards and methodologies, for its areas of responsibility, throughout the Cogne Group companies.

## 7.7.3 Health, Safety and Environment

The Health, Safety and Environment (HSE) Function:

- Ensures compliance with all obligations related to Workplace Health and Safety, Environmental Protection, Major Accident Prevention, and Fire Prevention.
- Ensures that all essential processes for managing health and safety risks and opportunities, Major Accident law obligations, and environmental matters are mapped and governed through appropriate procedures.
- Promotes a culture of Health and Safety and Environmental Protection by fostering constant cooperation among internal departments and engagement with external authorities, as well as encouraging an innovative approach.
- Manages all requirements related to the Occupational Health and Safety and Environmental Management System (ISO 45001 and ISO 14001 certified).

- Analyzes and verifies current legislation on Health and Safety, Environmental Protection, Major Accident and Fire Prevention, and ensures corporate compliance in the case of new obligations;
- Identifies risks, assesses them, and determines safety measures for workplaces, also in relation to planned plant, process, or management changes, and proposes preventive and protective measures to the Employer.
- Manages plant emergency response activities.
- Manages inspections and site visits by supervisory authorities (e.g., ARPA, USL, Fire Fighters, Labour Inspectorate, Environmental Unit, etc.);
- Directs and coordinates all internal HSE service activities, including training and professional development of its staff; it promotes the professional growth of personnel within a logic of continuous improvement aimed at achieving the company's strategic goals, while ensuring respect for safety regulations and specific safety measures.
- Verifies that all prescriptions issued by supervisory bodies and included in environmental, health and safety, and major accident prevention permits are correctly managed and complied with.
- Analyzes accidents, incidents, and near misses related to HSE and Seveso and proposes preventive and protective measures derived from such evaluations, as well as potential improvement actions.
- Reports and provides HSE and Major Accident data to internal departments upon request.
- Ensures the dissemination of shared standards and methodologies, for its areas of responsibility, throughout the Cogne Group companies.

## 7.7.4 Quality Assurance

The Quality Assurance Function:

- Manages all requirements related to the quality management system (certified under various standards, including ISO 9001, IATF 16949, EN 9100).
- Manages classification, the repository, and distribution of documents within the company's regulatory system, including those related to the Organization, Management and Control Model pursuant to Legislative Decree 231/01.
- Ensures the updating of system documents and supports the internal departments involved;
- Trains internal personnel responsible for conducting audits.
- Prepares the audit plan for second-level verifications, defines audit methods, selects auditors, and supports them in carrying out audits, if necessary.
- Evaluates, together with each auditor, any corrective actions to be undertaken by departments subject to audit.
- Develops the improvement plan and defines implementation deadlines for corrective actions in agreement with the relevant departments.
- Collects and reports, for the management review process, on the activities performed and the data instrumental to evaluating system performance.
- Processes data on internal and external non-conformities and communicates it to the relevant/requesting parties for reporting purposes.
- Verifies and manages updates to applicable standards by acquiring and storing them in the central repository.
- Plans and manages external audits, including those by certification bodies, customers, or supervisory entities.
- Coordinates product certification activities.
- Ensures the dissemination of shared standards and methodologies, for its areas of responsibility, throughout the Cogne Group companies.

## 7.7.5 Management Control

The Management Control Function:

- Supports top management in defining medium- to long-term strategic objectives based on past performance trends.
- Coordinates and oversees the strategic planning process to achieve Cogne Group's medium-term objectives (Business Plan).
- Coordinates and oversees the planning process to achieve short-term objectives of the Cogne Group (Budget).
- Defines performance measurement indicators
- Systematically collects and analyzes data related to company activities using specific systems and software.
- Prepares reports on the company's economic and financial performance.
- Oversees the entire investment process, calculating, for the most significant investments, expected ROI and payback period.
- Ensures compliance with deadlines and accuracy in the periodic reporting required by Management.

## 7.8 The Third Level of Control: Internal Audit

The Internal Audit Department of the Cogne Group is responsible for third-level control activities and is tasked with verifying that the ICS is functioning, adequate, and aligned with the strategic guidelines defined by the Board of Directors.

The Internal Audit Department:

- Defines the methodologies and operational processes for internal auditing, in accordance with the elements of the International Professional Practices Framework, the relevant guidelines, and best practices, and in line with the standards set by Walsin Lihwa Corporation.
- Prepares the Cogne Group's risk-based Audit Plan on an annual or multi-year basis, evaluating updates as needed based on emerging risks.
- Carries out and/or oversees the execution of the activities included in the Audit Plan, as well as any extra-plan activities.
- Provides support to the Governance, Control, and Supervisory Bodies of the Cogne Group, including through specific tasks, to assist them in fulfilling their duties.
- Periodically informs senior management and the Governance, Control, and Supervisory Bodies of the Cogne Group about the results of the audit activities carried out, any additional investigations performed, and the outcomes of the monitoring of the corrective actions identified.
- Oversees the monitoring of the implementation status of corrective actions resulting from its activities.
- Prepares an annual report for the Board of Directors of Cogne Acciai Speciali S.p.A. evaluating the Company's Internal Control and Risk Management System
- Prepares, when requested, reports on particularly significant events.
- Keeps the Walsin Lihwa Corporation Internal Audit function informed and aligned on the performance of activities.
- Oversees the management of whistleblowing reports, in compliance with legal requirements and the company's regulatory system.
- Is a member of the Supervisory Body of Cogne Acciai Speciali S.p.A. and therefore performs control and supervisory functions, including with the support of relevant company departments for updating Model 231.

## 7.8. IMPLEMENTATION OF THE INTERNAL CONTROL SYSTEM

The implementation of the Internal Control System (ICS or ICSRM) in a steel manufacturing context requires a structured and integrated approach that enables the prevention, identification, and management of risks associated with complex industrial activities, energy-intensive production processes, and regulatory compliance in the areas of environment, workplace safety, and product quality.

The system is inspired by international standards such as the COSO – Internal Control Integrated Framework and ISO 31000:2018 on Risk Management, which provide a well-established methodological framework to ensure the effectiveness, transparency, and resilience of business processes.

### 8.1 Definition of the Risk Appetite Framework

The Risk Appetite Framework ("RAF") defines the reference structure that outlines the company's risk appetite, tolerance thresholds, risk limits, risk governance policies, and the reference processes necessary to define and implement them, in line with the maximum acceptable risk, the business model, and the strategic plan. Its objectives are to:

- Connect governance, management, and control systems.
- Serve as a strategic control tool capable of linking risks to business strategy, as well as a management and risk control tool capable of aligning risk objectives with business operations.
- Act as a guiding tool for the risks undertaken and to be undertaken.

The fundamental elements of the RAF are:

- Risk Appetite: the level of risk the Company is willing to accept in pursuit of its strategic objectives.
- Risk Tolerance: the maximum deviation from the risk appetite that is allowed, where the tolerance threshold is set to ensure that the company can continue to operate within the maximum acceptable risk level, even under stress conditions.
- Risk Profile: the actual level of risk assumed, measured over a given time period.
- Risk Limits: quantitative measures based on forward-looking assumptions that allocate aggregate risk across individual entities, business lines, risk categories and/or other levels, according to the company's needs.

### 8.2 Context Analysis

Once the RAF is defined, context analysis becomes particularly significant in the steel industry, as the company operates in an environment characterized by high volatility in global raw material markets, significant environmental impacts, risks related to worker health and safety, and stringent regulatory compliance requirements.

The external context analysis includes factors such as steel price trends, European and national regulations on emissions and waste, and geopolitical tensions affecting the supply chain. The internal context analysis concerns production organization, technologies used, cost structure, plant management, and corporate culture regarding safety and quality.

## 8.3 Risk Taxonomy

Following the context analysis, the Risk Universe is constructed, which is understood as the definition of the categories of risks relevant to the Company. Specifically, the Risk Universe of the Cogne Group includes:

- Strategic risks.
- Financial risks.
- Operational risks.
- Compliance risks.
- External risks.

## 8.4 Risk Mapping and Analysis

Starting from the mapping of industrial and support processes (e.g., raw material procurement, melting, rolling, heat treatment, internal logistics, maintenance, quality, HSE), specific risks are identified for each process. These risks may fall into the categories and include, by way of example and not exhaustively:

- Governance, Reputation/Brand, Strategic initiatives, etc.
- Market, Liquidity, Credit, etc.
- Health and Safety, Environment, People, Product, Business Continuity, IT Systems, Fraud, etc.
- Legal, Non-compliance with internal regulations, Non-compliance with external regulations.
- Natural Events/Climate Change, Economic and/or Geopolitical Changes, Competition, Regulatory Evolution, etc.

The mapping of Health and Safety at Work, Environmental, Cybersecurity, Fraud, and other risk types is based on findings from in-depth vertical assessments, which also form the foundation of other management systems or models in place. With specific reference to fraud risk, fraud is defined as the abuse of one's role for personal gain through the misuse of corporate assets and resources. This category includes schemes related to corruption, embezzlement, and financial statement fraud.

## 8.5 Definition of Evaluation Metrics

Starting from the mapping of industrial and support processes (e.g., raw material procurement, To ensure consistency in risk assessment, structured and sector-appropriate measurement metrics are defined. The main metrics adopted include:

- Probability of occurrence: historical frequency of the event, temporal probability of the event occurring or recurring.
- Impact: financial loss, production downtime, impact on people and the environment, reputational damage.
- Existing control measures: technical (e.g., sensors, automation), organizational (e.g., procedures, maintenance plans), legal/contractual measures.

## 8.6 Risk Assessment

The definition and shared understanding of evaluation metrics allow for a risk assessment that is specific to the organization. Each risk is assessed in terms of:

- Potential Risk (gross of controls); and
- Residual Risk (net of controls, i.e., the level of risk remaining after controls have been applied), which is used to define intervention priorities.
- Existing control measures: technical measures (e.g., sensors, automation), organizational measures (e.g., procedures, maintenance plans), legal/contractual measures.

The assessments are presented using visual risk matrices, which facilitate communication and cross-functional understanding of risk levels and mitigation needs.

## 9. COMMUNICATION AND INFORMATION

The set of interrelations between the governing bodies, control functions, and management of Cogne Acciai Speciali and its directly controlled companies represents one of the fundamental operational mechanisms of the ICSRM.

For this reason, to enable the various stakeholders involved in the ICSRM to effectively perform their roles within the system, minimum information flows are defined between the different levels of control and the relevant management and control bodies, specifying their content and timing.

Company	Document	Responsible for Information Flow	Description	Frequency	Recipients
Cogne Acciai Speciali S.p.a.	Audit Plan	Internal Audit Department	The plan contains the schedule of audit activities based on a risk-based approach	Annual	Board of Directors CAS, Board of Statutory Auditors CAS, Supervisory Body CAS
Cogne Acciai Speciali S.p.a.	Audit Report	Internal Audit Department	The report contains the results of the audits in terms of: (1) objectives; (2) scope; (3) identified gaps and any remarks/areas for improvement; (4) defined corrective actions (including deadlines and responsible persons)	Event-driven	CEO CAS, General Director CAS, Director of the audited Area
Cogne Acciai Speciali S.p.a.	Audit Report of directly controlled companies	Internal Audit Department	The report contains the results of the audits in terms of: (1) objectives; (2) scope; (3) identified gaps and any remarks/areas for improvement; (4) defined corrective actions (including deadlines and responsible persons)	Event-driven	CEO CAS, GD CAS, CAS Director of the audited Area, CEO/GM of the controlled company, Board of Directors of the controlled company (case by case), Control Body (if required by local law)



Company	Document	Responsible for Information Flow	Description	Frequency	Recipients
Cogne Acciai Speciali S.p.a.	Corrective Actions Status Report	Internal Audit Department	List of defined corrective actions (including deadlines and responsible persons, status of progress) resulting from audit activities	Quarterly/ Event-driven	ICS, Risk Management and Compliance, CEO/GD CAS and/or controlled company (if necessary), Responsible persons for the corrective actions (if necessary)
Cogne Acciai Speciali S.p.a.	Risk Assessment Results	ICS, Risk Management & Compliance Department	Report containing the outcomes of Risk Assessment activities	Annual	CEO CAS, GD CAS, IA, Board of Directors CAS
Cogne Acciai Speciali S.p.a.	Results of second-level audits	ICS, Risk Management & Compliance Department	The report contains the results of second-level verification activities in terms of: (1) objectives; (2) scope; (3) identified gaps and any remarks/areas for improvement; (4) defined corrective actions (including deadlines and responsible persons)	Annual / Event-driven	IA, CEO/GD CAS (for anti-corruption audits), Board of Directors CAS (for anti-corruption audits)

# 10. MONITORING AND REPORTING

The continuous monitoring of the internal control system is carried out through internal audits, performance indicators (KPI/KRI), operational control activities, and periodic information flows. In the steel industry, monitoring is crucial for preventing high-impact events such as serious accidents, environmental non-compliance, or production disruptions.

The reporting of monitoring results is structured to reach both operational levels and top management, ensuring transparency, timeliness, and support for decision-making. These information flows are integrated into the cycle of review and update of the system, in line with the principle of continuous improvement, ensuring the dynamic evolution of controls in response to new threats or changes in the context.

## 10.1 ICS Evaluation

The periodic evaluation of the adequacy and effective operation of the ICS, as well as its possible revision, is an essential part of the ICSRM structure, aimed at ensuring its full and proper effectiveness. This responsibility lies with the Board of Directors, supported by the Chief Executive Officer/General Manager.

In conducting this activity, the Board of Directors will not only verify the existence and implementation of the ICSRM within the company but also periodically carry out a detailed review of the system's structure, its suitability, and its actual and concrete functioning.

Additionally, every year, during the meeting to approve the draft financial statements, the Board of Directors is required to:

- Examine the significant business risks presented by the CEO and assess how those risks were identified, evaluated, and managed. Particular attention should be paid to changes that occurred during the reference financial year, in the nature and extent of the risks, and in the company's response to such changes.
- Evaluate the effectiveness of the ICSRM in dealing with these risks, focusing on any reported inefficiencies.
- Examine which actions have been implemented or need to be promptly undertaken to address the identified inefficiencies.
- Promote the adoption of additional policies, processes, and procedures that enable the company to respond appropriately to emerging risks or those not adequately managed.

## 10.2 Continuous Improvement

The continuous improvement of the ICS is achieved through the monitoring activity of the system itself. Monitoring involves all activities aimed at verifying that the ICS is properly designed and operational. It is carried out through ongoing supervision, periodic assessments, or a combination of both.

Supervision is implemented within the context of daily operations and includes routine monitoring activities performed by various company roles, through initiatives carried out as part of their assigned duties.

Periodic assessments are conducted based on risk evaluation and the effectiveness of the supervision procedures.

Continuous improvement must be considered an integral part of regular operational activities.

## 11. REVIEW OF THE GUIDELINES

The Cogne Group commits to updating the Guidelines as needed due to changes in context, laws, environment, or organizational structure.



