FEDRIGONI

ENTERPRISE RISK MANAGEMENT POLICY

1. PURPOSE AND SCOPE

Risk is an **integral part of doing business.**

Every choice in pursuing business objectives has its risks: **from day-to-day operations to strategic decisions**. Since dealing with risk is embedded in the decision-making process, there is no growth or value creation without taking risks.

Therefore, considering the increasingly uncertain, dynamic and complex business context, **the Group has decided to implement an Enterprise Risk Management** (*hereinafter referred to as ERM*) **Model** for the systematic assessment, management and monitoring of business risks, as a sound and robust way to run business and achieve long-term performance objectives.

RISK is any uncertain event that could THREATEN the achievement of BUSINESS OBJECTIVES and STRATEGIES or the company's tangible and intangible ASSETS

The goal of this document **is to define the Risk governance framework** and **providing guidelines for identifying, evaluating, managing and monitoring risks** that could threaten the Group's ability to deploy its strategies and optimize performances.

More in detail, the **purpose** of this policy is to **set-out**:

- the **mission** of the Group's **ERM Model**
- the **Governance Model** describing roles and responsibilities of the main parties involved
- the **ERM process**, in terms of activities to be performed on a regular basis and supporting methodologies

2. MISSION OF THE ERM MODEL

ENTERPRISE RISK MANAGEMENT

The culture, capabilities, and practices, integrated with strategy setting and execution, that organizations rely on to manage risk in creating, preserving, and realizing value[1]

[1]COSO ERM FRAMEWORK: "Enterprise Risk Management Integrating with Strategy and Performance", 2017.

The **mission of the ERM model** is to:

- Provide the Management and the Board with a **view of the main risks** the Group is exposed to and a clear **understanding of their impacts** on Group's objectives
- **Ensure** that **appropriate risk management strategies** are **defined and enforced to address / mitigate the main risks**
- **Improve the Group capabilities** to anticipate and/or respond to business changes and uncertainties, focusing on the risks that can impact strategies and performance.

- **Enhance the capability to achieve long-term performance** objectives, thus increasing opportunities and creating corporate value
- **Set a common risk language within the organization**, enabling management with heterogeneous backgrounds and experiences to communicate more effectively on different risk issues.

3. ERM GOVERNANCE

The **Fedrigoni's ERM Governance model** sets out roles & responsibilities integrating different levels of controls ensuring that all risks are effectively addressed and communicated within the organization.

The model - aligned with the ERM best practices - is graduated according to the size and the organizational structure of the Group.
The **main parties involved** in the ERM process are:

BOARD OF DIRECTORS

Overall risk oversight

The Board of Directors is the primary responsible for supervising, addressing and assessing the Group ERM system by:

- **Overseeing** the **ERM system** so that **risks assumed** are **consistent** with **Group's strategies** and **with** the **nature** and **level of risk** the Group is willing to accept
- **Defining** the **ERM system guidelines** so that the main risks are correctly identified and adequately measured, managed and monitored
- **Evaluating**, at least on an annual basis, the **Risk Management system adequacy** and **effectiveness**

AUDIT & RISK COMMITTEE

Advisory to the board

The Audit & Risk Committee supports the Board of Directors in the decisions related to the ERM system. It is responsible for:

- **Annually reviewing the organisation's risk profile**
- **Providing oversight** on **significant risk exposures** and eventually ask for further analysis on Top Risks
- **Reviewing** and **providing advice** on the risk **management process** and the **procedures in place**

CEO

ERM strategy definition and implementation

The Chief Executive Officer is responsible for establishing and maintaining an effective ERM system by:

- **Implementing** the **guidelines defined by the Board of Directors**, overseeing the ERM system design and implementation

	• **Ensuring leadership** and **commitment** with respect to ERM system • **Discussing** and **approving risk assessment results** and **risk management strategies** and related ownerships • **Ensuring** that the most **relevant risks** and **related risk management strategies** are periodically **reported to the Board** • **Approving** the **ERM approach**, **methodology** and **supporting tools** and **their update**
EXECUTIVE COMMITTEE	The Executive Committee, supports the CEO by **carrying out** evaluations and decisions regarding the ERM system
INTERNAL AUDIT, RISK & COMPLIANCE *Risk facilitation, methodological support, coordination & reporting*	The Internal Audit, Risk & Compliance, when in charge of Risk Management responsibilities: • **Define**, **implement** and **maintain appropriate processes**, **tools** and **methodologies** for dealing with business risks • **Facilitate** the **identification**, **assessment** and **management** of **business risks** • Periodically **report on risks** to the **CEO** and the **Audit & Risk Committee** and **share the results** with the **Executive Committee** • **Monitor** - on a regular basis - the Group **risk profile** evolution and **risk mitigation action plans** • **Provide input for the risk-based Audit Plan** so that audit activities could be planned considering the Enterprise Risk Assessment priorities
Independent assurance	The Internal Audit, Risk & Compliance, when in charge of Internal Audit responsibilities provide **assurance** on the overall **effectiveness** and **adequacy** of the Group Internal Control and Risk Management system
MANAGEMENT *Risk identification, assessment and management*	Management, who have day-to-day ownership and accountability for identifying, assessing and managing risks - i.e. Risk Owners -, are responsible for: • **Identifying, evaluating** and **managing risks according to their area of competence** and **defined ownership**

- **Proposing, implementing** and **monitoring risk mitigation action plans to maintain an acceptable risk exposure**

4. ERM PROCESS

The Fedrigoni ERM process consists of **4 main phases**:

- **Risk Assessment** - *identification and evaluation*
- **Risk Response**
- **Risk Monitoring**
- **Risk Reporting**

4.1 RISK ASSESSMENT

RISK IDENTIFICATION & EVALUATION

Risk Identification aims at detecting and describing relevant risk events that could affect the Group's ability to achieve its objectives, effectively perform operations and create sustainable value.

Risk identification is performed at least annually involving **Key Managers** and any level of the organization which could provide valuable contribution to risk understanding and context description.

Internal Audit, Risk & Compliance supports risk identification by providing risk knowledge based on past experience, previous risk analyses and business context, enabling discussion and brainstorming on risks through interactive meetings/interviews.

Each risk event should be classified according to Fedrigoni's Risk Model in order to grant a common risk language across the Group and to ensure all risk areas are explored through a consistent process.

According to the **Group Risk Model**, the identified risks are classified into the following **Risk Categories**:

Strategic Risks: risks related to the external business environment as well as to internal strategy and governance decisions that might significantly affect Group's performances and /or the achievement of strategic goals.

Operational Risks: risks that may affect the effectiveness / efficiency of business processes, with negative effects on value creation.

Financial Risks: risks related to exchange rate, interest rate, credit, capital availability, liquidity, etc. not effectively managed.

Legal & Compliance Risks: risks of non-compliance with existing laws and regulations as well as internal policies and procedures which may lead to litigations, penalties and potential negative effects on Group's reputation.

Each identified risk is assessed and **prioritized according** to the following **evaluation criteria**:

Quali-quantitative impact *(Economic, Reputational, Operational, HSE & Sustainability)*

Likelihood of occurrence over the risk assessment timeframe

The maturity level of the existing Risk Management system

At the end of the identification & evaluation phase, each risk is plotted on a chart (Risk Heatmap) according to its value of likelihood of occurrence and impact

4.2 RISK RESPONSE

Risk Response phase aims at defining the appropriate countermeasures to avoid, reduce or transfer identified risks, leading Group risk exposure to an acceptable level. It consists in selecting the most appropriate risk mitigation strategy and defining related action plans.

The **risk management strategies** which can be adopted to reduce risk exposures aligning them with the desired levels are described below:

- **AVOID** risk by ceasing a particular activity or by reconsidering objectives
- **REDUCE** probability of occurrence and/or impact of an adverse event by proactively define countermeasures
- **TRANSFER/SHARE** risk exposure through insurance contract, physical or financial hedging, process outsourcing
- **ACCEPT** risk at its present level taking no further action and focusing on monitoring activities

Internal Audit, Risk & Compliance ensures that the activity is performed for all relevant risks, supporting Risk Owner in defining useful methods to address/mitigate them.

4.3 RISK MONITORING

Risk Monitoring aims at ensuring a **regular monitoring** of:

- The **evolution** of **Top Risk exposure**, in terms of likelihood of occurrence and impact in order to understand if risk exposure is worsening and promptly address the risk whenever deemed necessary.
- Risk **response implementation status** and **effectiveness** in order to understand if further countermeasure shall be implemented.

Risk monitoring activities are performed **continuously throughout the year** aimed to evaluate the progress status of approved action plans

4.4 RISK REPORTING

Risk Reporting is performed at least annually by Internal Audit, Risk & Compliance and it is aimed at **disclosing the outcomes of the ERM activities** to the **CEO**, the **Executive Committee** and the **Audit & Risk Committee** in order to provide them with a complete view of the main risks the Group is exposed to.

GLOSSARY

ERM Governance Model	Model describing the organizational structure, Board oversight, Management roles, responsibilities and accountabilities in relation with the development, implementation and maintenance of Enterprise Risk Management processes.
Group Risk Model	The risk universe encompassing potential risks the Group may face when performing its business activities. It is a system aimed at facilitating Management discussions on risks by introducing/setting a common risk language.
Heat Map	Likelihood of occurrence and impact chart used to graphically represent risk analysis results in a meaningful and concise way. Each risk is plotted on the chart prioritizing them according to its value of likelihood of occurrence and impact.
Likelihood of Occurrence	Probability that the risk event may occur over a given timeframe.
Risk	Potential future event that may have a negative impact on Fedrigoni's objectives and results, as well as on Group key value drivers.
Risk Impact	Estimated loss in case of risk occurrence. It can be expressed in terms of economic (i.e. EBITDA), financial (i.e. CF), operational, reputational, HSE effects.
Risk Owner	Management responsible for setting and coordinating risk management guidelines on specific risk, considering business objectives and budget limits. The Risk Owner is responsible for risk management activities and has the authority and competences to ensure an effective risk identification, management and monitoring.
Risk Strategy	Strategic decisions to address risk exposure taking into consideration the extent and nature of risks the Group is willing to take in pursuing its objectives.