



Risk Management Policy and Governance Model

Contents

1. Purpose	2
2. Scope of application	3
3. Governance model: Responsibilities within the Risk Management System	3
4. The process	5
4.1. Identification of risks	5
4.2. Risk assessment	6
4.3. Risk management.....	7
4.4. Risk monitoring	7
4.5. Updating and monitoring.....	7
4.6. Effectiveness of the Risk Management System.....	8

	RISK CONTROL AND MANAGEMENT POLICY	Code:	
		Edition:	00
		Page:	2 of 8

1. Purpose

This document serves to set out the risk control and management policy in place at SIDENOR ACEROS ESPECIALES, S.L.U. (hereinafter called "SIDENOR") to provide a general framework for action and establish procedures and responsibilities in effectively and efficiently controlling and managing the risks faced by the company.

SIDENOR's Risk Management System (RMS) provides the company with reasonable assurances that all significant risks (be they strategic, operational, financial, compliance-related or governance-related) are envisaged, identified, assessed, continually monitored and kept at appetite and tolerance levels low enough to secure the approval of the company administration.

With strong, sustained commitment on the part of the Executive Committee of the group and stringent strategic planning, the aim is to provide an environment where risks can be worked with in a controlled fashion and managed actively so that new opportunities can be seized.

The RMS is based essentially on the following principles:

- Fostering a constructive vision of the concept of risk.
- Commitment and competency on the part of the persons involved.
- All speaking the same language.
- Transparency in communication throughout the organisation.

SIDENOR personnel with responsibility for the RMS are provided with the human and material resources needed to perform their functions properly.

In this policy document, SIDENOR sets out guidelines for identifying risks and keeping them below the tolerance levels approved from time to time by the company administration.

The procedures for implementing this policy must be consistent with the principles and guidelines set out here, which seek to do the following:

- to help attain the company's strategic goals;
- to provide the greatest possible assurances in terms of safeguarding the interests of the company and thus of all its shareholders and other stakeholders;
- to protect the reputation of SIDENOR;
- to safeguard SIDENOR's stability and financial soundness as a business in a sustained fashion;
- to help ensure compliance with regulations;
- to help ensure that operations take place in line with the safety and quality terms agreed.

Issued & reviewed by: Head of Risk Management	Approved by: Company administration	Date: November 2019
----------------------------------------------------------	--------------------------------------------	----------------------------

	RISK CONTROL AND MANAGEMENT POLICY	Code:	
		Edition:	00
		Page:	3 of 8

In line with the above, this policy is grounded on the following basic principles:

- **Fostering a risk-management-oriented approach** from the drawing up of strategies and risk appetites to the factoring of the relevant variables into operational decisions.
- **Breaking down responsibilities & allocating them** to areas that take risks and to those charged with analysing, controlling and supervising those risks, and seeking to ensure that the most effective risk hedging instruments are used.
- **Providing clear information** on risks at the group and on the operation of control systems, via approved communication channels.
- **Ensuring compliance with the regulations covering corporate governance and updating** those regulations as per international best practices in the relevant field, acting in line with the company's corporate governance rules at all times.

2. Scope of application

This policy applies to SIDENOR's RMS at all its plants and investee companies and in all areas. It covers risks involving financial and non-financial information that currently or may potentially affect SIDENOR, regardless of whether they arise from the company's activities or from elsewhere in its working environment.

3. Governance model: responsibilities within the Risk Management System

All members of the Executive Committee, senior management and other employees of SIDENOR are responsible for implementing this policy in their respective management areas and for coordinating actions in response to risks with other departments and management areas as relevant.

The various roles involved in SIDENOR's RMW can be grouped into three lines of defence against risks that threaten the attainment of strategic, operational, financial, compliance-related and governance-related goals.

1. First line of defence: SIDENOR's operational management. Responsible for assessing, controlling and mitigating risks and for setting up effective internal controls.
2. Second line of defence: SIDENOR's Risk Management Function (handled by the Head of Legal Advisory Services) and other areas concerned with internal control and compliance. This area must facilitate and supervise the implementing of effective internal controls and risk management practices.

Issued & reviewed by: Head of Risk Management	Approved by: Company administration	Date: November 2019
----------------------------------------------------------	--------------------------------------------	----------------------------

	RISK CONTROL AND MANAGEMENT POLICY	Code:	
		Edition:	00
		Page:	4 of 8

3. Third line of defence: Internal audits. This area must provide the company's governing bodies with assurances as to the effectiveness of internal controls and risk management, including the operation of the first and second lines of defence.

In this context, the roles and responsibilities of each member of the organisation involved in the RMS are as follows:

Body	Responsibilities
Company administration (Sole Administrator)	<ul style="list-style-type: none"> ✓ Ultimately answerable to shareholders for the existence and operation of the RMS.
Executive Committee	<ul style="list-style-type: none"> ✓ Identifying, assessing and managing risks (Risk Owners). ✓ Implementing and transmitting a risk-oriented culture in the company. ✓ Defining, setting and/or changing the risk appetite, with responsibility shared with the company administration, which must give its approval. ✓ Approving the risk map. ✓ Approving plans and actions proposed by Risk Owners and by the Head of the RMS as deemed necessary to tackle the risks identified. ✓ Assessment and supervision of SIDENOR's RMS.
Senior Management	<ul style="list-style-type: none"> ✓ Identifying, assessing and managing risks (Risk Owners). ✓ Implementing and transmitting a risk-oriented culture in the company.
Head of the Risk Management System	<ul style="list-style-type: none"> ✓ Designing & implementing the operation of the RMS. ✓ Drawing up SIDENOR's method, procedures and criteria for identifying, sorting, approving and responding to risks. ✓ Drawing up and updating the risk map. ✓ Reporting regularly to the Executive Committee on changes in risks over time and on the operation of the RMS in general.
Internal Audits	<ul style="list-style-type: none"> ✓ Assessing the effectiveness of the RMS and reporting regularly to the Executive Committee on any weaknesses detected and on the timetable for measures to correct them.
Other employees	<ul style="list-style-type: none"> ✓ Identifying any risks to fulfilment of their goals and for reporting same to their area heads. ✓ Working with area heads to assess and classify risks and propose action plans to tackle them, and helping to implement those plans.

Breakdown of RMS functions

	Company administration	Executive Committee	Management	Head of RMS	Internal Audits	Other employees
Identification of risks		X	X	X		X
Risk assessment		X	X	X		
Management of risks identified		X	X	X		
Risk monitoring	X	X		X	X	
Approval of RMS	X	X				
Updating of RMS		X	X	X		
RMS effectiveness assessment					X	

4. The process

SIDENOR defines "risk" as any event arising from internal or external factors that hinders or prevents the attainment of its strategic and operational goals.

The RMS adopted by SIDENOR is an integrated system that considers all significant risks of all kinds to which the company may be exposed, and particularly those that may affect the fulfilment of the Business Plan.

The RMS is based on the COSO ERM framework, adapted to the needs of SIDENOR. It entails the following main components:

4.1. Identification of risks

Risks are identified by looking for events (associated with internal or external factors) that could affect SIDENOR's goals in terms of strategic plans, corporate social responsibility and annual budgeting.

Understanding **external factors** is important for ensuring that the goals and concerns of stakeholders are taken into account. External context may include, but is not limited to, the following:

- a) The social, cultural, political, legal, financial, technological, economic, natural and competition-related context at international, national, regional and local levels.
- b) Factors and trends that impact the goals of the organisation.
- c) Relations with stakeholders.

Internal factors are those that the organisation can influence, and thus manage risk levels. The risk management process must be consistent with the culture, processes, structure and strategy of the organisation.

	RISK CONTROL AND MANAGEMENT POLICY	Code:	
		Edition:	00
		Page:	6 of 8

The risk category defined is as follows:

- **Strategic and planning risks:** Risks that affect high-level goals directly linked to the Strategic Plan.
- **Operational/infrastructure risks;** Risks that affect goals linked to the effective, efficient use of resources.
- **Financial (reporting) risks:** Risks that affect financial goals.
- **Compliance:** Risks of non-compliance with external or internal regulations on the part of the senior management or of employees.
- **Governance:** Risks affecting company, ethical and corporate-governance-related aspects and compliance with legislation and regulations.

4.2. Risk assessment

Scales have been drawn up to establish consistent criteria for assessing risks: **impact, likelihood & speed of occurrence**.

Impact is measured in five categories: effect on Strategic Plan goals, economic effects (EBITDA), reputational effects, regulatory effects & time dedicated by the Executive Committee.

Likelihood is the probability of occurrence of an event during the period covered by the Strategic Plan. It can be expressed in qualitative terms such as a percentage rate or in terms of frequency.

Speed of occurrence is the time that elapses from the appearance of the risk to the time when it directly or indirectly affects the goals of SIDENOR.

These scales serve to locate each risk on the **Risk Map**, which is the main risk assessment tool.

Risk assessment is the remit of the Executive Committee, senior management and the Head of the RMS, who must assess risks identified within set periods.

Once completed, their assessments are consolidated to form the Risk Map. In consolidating risks, the specific weights of the assessments by the above parties for each type of risk are taken into account so that an overview of SIDENOR's situation is drawn up that enables risks to be prioritised. This process is led by the Head of Risk Management.

In its RMS, SIDENOR distinguishes between **inherent risks** and **residual risks**. The difference between them is that residual risk is assessed taking into account controls and impact-reducing measures already in place, so it is lower or at least no higher than inherent risk.

SIDENOR's RMS also takes **planned residual risks** into account: these are defined as residual risks mitigated by additional controls or impact-reducing measures to be adopted in the short, medium or long term.

Issued & reviewed by: Head of Risk Management	Approved by: Company administration	Date: November 2019
----------------------------------------------------------	--------------------------------------------	----------------------------

	RISK CONTROL AND MANAGEMENT POLICY	Code:	
		Edition:	00
		Page:	7 of 8

4.3. Risk management

Once risks have been identified, assessed and consolidated, action plans must be drawn up to bring them down to levels acceptable to the organisation.

Organisations can implement the following actions or responses to risks:

- **Mitigation:** actions are taken to reduce the impact or likelihood of occurrence of a risk to bring it down to a level acceptable to the organisation.
- **Acceptance:** no action is taken in regard to a risk: its consequences and the likelihood of its occurrence are accepted as is.
- **Sharing:** actions are taken to share part of the risk with third parties, e.g. by taking out insurance, outsourcing certain processes, etc.
- **Avoidance:** risks are eliminated by suspending the activity that gives rise to them.

The risk manager must regularly monitor each risk identified, particularly critical risks, and analyse the potential for occurrence via suitable quantitative or qualitative indicators. If an indicator exceeds the tolerance level set, the risk manager must identify the causes and propose an action plan or response.

Responses to risks must be reviewed by the Head of the RMS, who must then report to the Executive Committee.

4.4. Risk monitoring

To ensure that the agreed responses to risks are viable and efficient, the Head of Risk Management conducts a monitoring study each year that covers the following points:

- ✓ Confirming that risks are being managed as approved by the Executive Committee.
- ✓ Assessing whether the agreed responses are efficient and setting up action plans if necessary.
- ✓ Checking whether the risk map anticipates and reflects any changes in the circumstances of the business and new economic conditions.

The Head of Risk Management must also determine whether any risks have actually materialised, and if so must check the measures adopted to mitigate them.

4.5. Updating and monitoring

Business risks change over time, so the RMS must be changed accordingly. Risks that were once critical may become less important, while others become more critical.

To keep the RMS effective and up to date, the Head of Risk Management must update the Risk Map every year via the process described above.

Issued & reviewed by: Head of Risk Management	Approved by: Company administration	Date: November 2019
----------------------------------------------------------	--------------------------------------------	----------------------------

	RISK CONTROL AND MANAGEMENT POLICY	Code:	
		Edition:	00
		Page:	8 of 8

The updated map must be submitted to the Executive Committee for review and approval.

The company administration is ultimately responsible for supervising the RMS.

4.6. Effectiveness of the Risk Management System

The Internal Audits area must provide the governing bodies with assurances as to the effectiveness of the RMS and of the checks and impact/likelihood reducing measures implemented. This includes analysing the workings of the first and second lines of defence and identifying recommendations that can strengthen the RMS.