



CIE Automotive

Risk Control and Management Policy

Contents

1. Purpose.....	3
2. Scope of application	4
3. Responsibilities.....	4
4. Description of the process	6
4.1. Identification of risks	6
4.2. Risk assessment	6
4.3. Risk management.....	7
4.4. Risk monitoring	7
4.5. Updating and monitoring.....	8
4.6. Breach	8

	RISK CONTROL AND MANAGEMENT POLICY	Code:	CIE CO CP PO 03
		Review:	04
		Page:	3 of 8

1. Purpose

The purpose of this document is to define the Risk Control Management Policy of CIE Automotive, S.A. ("**CIE Automotive**" or the "**Group**") to establish the general framework for action, as well as the procedures and responsibilities to control and manage the risks that CIE Automotive must face efficiently and effectively.

The risk management system of CIE Automotive ("**RMS**") allows it to reasonably ensure that all significant risks, both financial and non-financial risks, including those related to corruption, are prevented, identified, assessed, subjected to ongoing control and reduced to the defined levels of risk appetite and tolerance and are ultimately approved by the Board. CIE Automotive defines the following risk categories: strategic, operational, financial (see the policy on the Internal Control over Financial Reporting (ICFR) Policy), compliance and ESG (Environmental, Social and good Governance).

With a strong and sustained commitment of senior management and the management team, as well as rigorous strategic planning, the Group aims to achieve an environment where it is capable of working with risks in a controlled manner, managing them actively and, thereby, take advantage of new opportunities.

The principles on which it is based are fundamentally:

- ✓ To promote a constructive vision of the concept of risk.
- ✓ Commitment and competence of participants.
- ✓ To use a common language.
- ✓ Transparent communication throughout the organisation.

CIE Automotive employees with RMS-related responsibilities will have the material and human resources necessary to perform their functions.

Through this Policy, CIE Automotive defines the guidelines to follow to identify and maintain the risks within the tolerance limits approved at any given time by the Board.

The procedures developed by this Policy must be consistent with the principles and guidelines established here that are aimed at:

- ✓ Contributing to achieving the strategic objectives of the Company.
- ✓ Introducing maximum guarantees in relation to the protection of corporate interests and, therefore, all shareholders and other stakeholders.
- ✓ Protecting the reputation of CIE Automotive.
- ✓ Safeguarding the business stability and financial solidity of CIE Automotive in a sustainable manner.
- ✓ Contributing to complying with the regulations.
- ✓ Facilitating the performance of transactions under the conditions of security and quality undertaken.

In accordance with the foregoing, this Policy is based on the following basic principles:

- ✓ Promoting an approach to risk management that ranges from defining the strategy and risk appetite, to incorporating the aforementioned variables into operational decisions.
- ✓ segregating and assigning responsibilities to the risk-taking areas and those in charge of its analysis, control and supervision, as well as seeking to guarantee the use of the most effective instruments to hedge risks.
- ✓ Reporting transparently on the risks of the Group and the functioning of the control systems through the approved channels of communication.

Issued and reviewed: Audit and Compliance Committee	Approved: Board of Directors	Date: October 2020
--	-------------------------------------	---------------------------

- ✓ Ensuring compliance with the corporate governance rules and ensuring that the aforementioned rules are updated in accordance with international best practices in relation to the matter, acting at all times in accordance with the Company's corporate governance regulations.

2. Scope of application

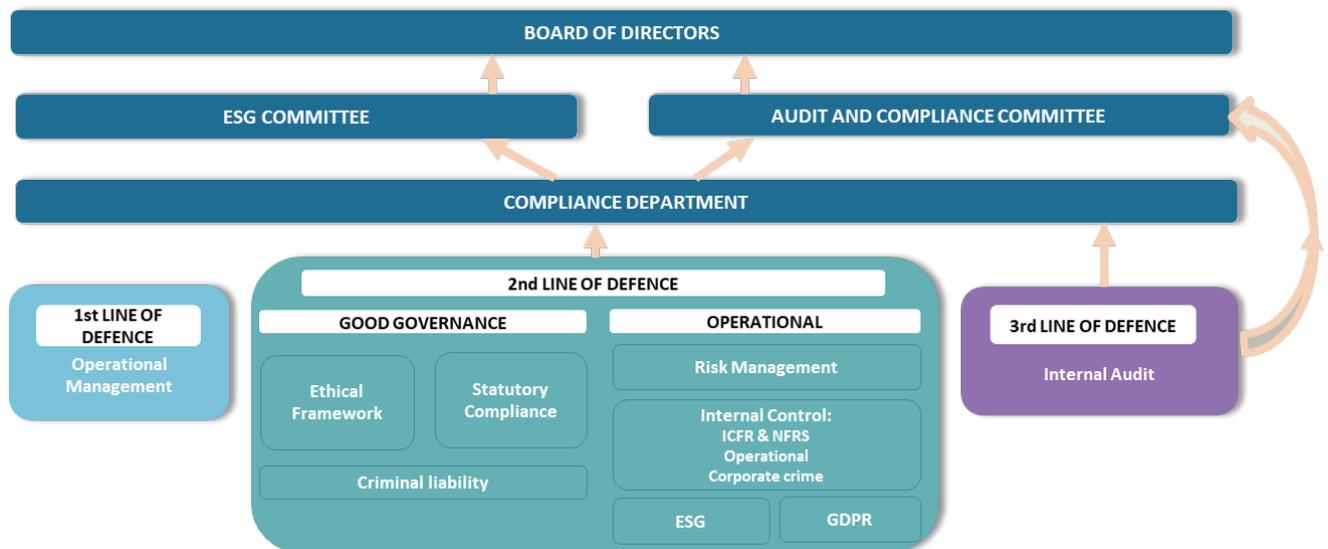
This policy is applicable to the RMS of CIE Automotive in all of its centres, investees and areas, covering all the risks regarding financial and non-financial reporting that affect or may affect CIE, whether they arise from its environment or from its activities.

3. Responsibilities

CIE Automotive Board members, its management team and all employees are responsible for implementing this policy within their scope of management and to coordinate their responses to the risks with the other managers and departments affected, where applicable.

The various roles involved in the RMS may be grouped into three lines of defence against the risks that threaten fulfilment of the strategic, operational, financial and ESG objectives. Although the first line of defence reports directly to senior management and the management team, both the second and third lines of defence report to the Compliance Department.

As shown in the accompanying chart, in RMS the three lines of defence are supervised by the Board¹:



¹ ICFR: Internal Control over Financial Reporting
NFRS: Non-Financial Reporting Statement
GDPR: General Data Protection Regulation
ESG: Environment, Social & Governance

	RISK CONTROL AND MANAGEMENT POLICY	Code:	CIE CO CP PO 03
		Review:	04
		Page:	5 of 8

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

Body	Responsibilities
Board of Directors	<ul style="list-style-type: none"> ✓ The Board of Directors is ultimately responsible to the shareholders for the existence and operation of the RMS. ✓ Supervision of the RMS through the activities carried out by the Audit and Compliance Committee.
Audit and Compliance Committee	<ul style="list-style-type: none"> ✓ Assessment and supervision of the RMS of CIE. ✓ Informing the Board of the results of the assessments carried out and the schedule assigned to the measures proposed for the weaknesses detected.
Senior Management and Management Team	<ul style="list-style-type: none"> ✓ Responsible for identifying and assessing the risk. ✓ Implementing and spreading a culture focused on risk at the Company. ✓ Defining, establishing and/or modifying the risk appetite that will be shared with the Board for its approval. ✓ Approving the plans and actions proposed by the Compliance Department that may be considered necessary to handle the risks identified.
Compliance Department	<ul style="list-style-type: none"> ✓ Responsible for designing and implementing the operation of the RMS. ✓ Defining the methodology, procedures and criteria of CIE Automotive for identifying, assessing, classifying, approving and responding to risks. ✓ Responsible for preparing the Risk Map. ✓ Periodically reporting to the Audit and Compliance Committee regarding the evolution of the risks, as well as the general operation of the RMS.
Cross-Group ESG Committee	<ul style="list-style-type: none"> ✓ Responsible for identifying and assessing the risk. ✓ Implementing and spreading a culture focused on risk at the Company. ✓ Approving the plans and actions proposed by the Compliance Department that may be considered necessary to handle the risks identified.
Internal Audit Department	<ul style="list-style-type: none"> ✓ Assessing the efficacy of the RMS and periodically reporting to the Audit and Compliance Committee and senior management and the management team the weaknesses detected and the schedule established for implementing measures to correct them.
Other employees	<ul style="list-style-type: none"> ✓ Responsible for identifying risks that threaten fulfilment of its objectives and communicating them to the head of the area. ✓ Collaborating with the area heads in the assessment and classification of the risk, as well as proposing action plans to address the risks identified and collaborate on the execution thereof.

RMS segregation of duties matrix:

	Board of Directors	Audit and Compliance Committee	Senior Management and Management Team	Compliance Department	Internal Audit Department	Cross-Group ESG Committee	Other employees
Identification of risks		X	X	X		X	X
Risk assessment			X	X		X	
Risk management				X			
Risk monitoring	X	X		X	X		
Update			X	X		X	
Breaches					X	X	X

Issued and reviewed: Audit and Compliance Committee	Approved: Board of Directors	Date: October 2020
--	-------------------------------------	---------------------------

	RISK CONTROL AND MANAGEMENT POLICY	Code:	CIE CO CP PO 03
		Review:	04
		Page:	6 of 8

4. Description of the process

CIE Automotive defines risk as any event, caused either by internal or external factors, that hinders or impedes the achievement of its strategic and operational objectives.

The RMS adopted by CIE Automotive is comprehensive and takes into account all the significant risks of any nature to which it may be exposed and, in particular, those that may affect fulfilment of the Business Plan.

The RMS is based on the methodology of ISO 31000 and adapted to the needs of CIE Automotive. It uses the SAP GRC risk management software for support and in it the following main components are defined:

4.1. Identification of risks

The risk identification process consists of searching for events (associated with internal and external factors) that may affect the objectives of CIE Automotive, both of the Strategic Plan and the ESG Business Model, as well as the annual budget.

It is important to understand the **external factors** to ensure that stakeholders' objectives and concerns are taken into account. The external context may include, but is not limited to:

- a) The social, cultural, political, legal, financial, technological, economic, natural and competitive environment at the international, national, regional or local level.
- b) The factors and trends that have an impact on the organisation's objectives.
- c) Stakeholder relations.

Internal factors are those on which the organisation may have an influence and, consequently, manage the risk. The risk management process must be consistent with the culture, processes, structure and strategy of the organisation.

The risk categories defined are the following:

- **Strategic:** risks that affect the high-level objectives directly related to the Strategic Plan.
- **Operational:** risks that affect the objectives related to the effective and efficient use of resources.
- **Financial:** risks that affect the financial objectives.
- **Compliance:** risk of management or employees breaching external and internal regulations.
- **ESG (Environmental, Social and Governance) Risks:** Risks that affect environmental, social, ethical and corporate governance matters and compliance with laws and rules.

4.2. Risk assessment

With the goal of defining homogeneous criteria for assessing risks, assessment scales have been defined: probability of occurrence and impact, where the impact is measured in three categories: economic, organisational and reputational. These scales serve to locate each risk and the Risk Map, the main tool for assessing risks.

When assessing risk, the speed of occurrence is also considered. This is defined as the time that elapses from the materialisation of the risk until it directly or indirectly affects the objectives of CIE Automotive.

In addition to defining the assessment scales for each risk, the following aspects will be defined:

- a) Source of the risk.
- b) Identification of the areas of impact of the risk, i.e., define, in the event of occurrence, in what way it would affect the Company.

Issued and reviewed: Audit and Compliance Committee	Approved: Board of Directors	Date: October 2020
--	-------------------------------------	---------------------------

	RISK CONTROL AND MANAGEMENT POLICY	Code:	CIE CO CP PO 03
		Review:	04
		Page:	7 of 8

c) Identification of the parties responsible for managing risks.

The risk assessment process is the responsibility of senior management and the management team who will have to assess the risks identified in the periods established.

Once the assessments are obtained, they will be consolidated to obtain the Risk Map. The consolidation of the risks will take into account the specific weight of the assessments of each one of the parties responsible and of each geographic area for each type of risk so that it provides a global vision of CIE Automotive and enables them to be prioritised. This process is carried out by the Compliance Department.

4.3. Risk management

Once the risks have been identified, assessed and consolidated, the action plans to reach the risk level accepted by the organisation must be determined.

The actions or responses to the risk that the organisation may adopt are the following:

- ✓ **Mitigation:** actions aimed at reducing the impact or the probability of occurrence of the risk to a level acceptable to the organisation.
- ✓ **Acceptance:** no actions taken in relation to the risk in question. The consequences of the risk and their probability of occurrence are accepted.
- ✓ **Sharing:** actions aimed at sharing a portion of the risk with third parties, for example, through arranging insurance, outsourcing processes, etc.
- ✓ **Avoidance:** suspending the activity that gives rise to the risk so that it ceases to exist.

For each one of the risks identified, in particular for the critical risks, the manager of the risk will periodically monitor them and analyse their possible materialisation through appropriate quantitative or qualitative indicators. If an indicator exceeds the established tolerance, the risk manager will be in charge of identifying the causes and proposing an action plan or response.

The Compliance Department is responsible for the process of reviewing the responses to the risks and afterwards it will present it to the Audit and Compliance Committee.

4.4. Risk monitoring

To ensure that the responses to the risks agreed are viable and efficient, the Compliance Department will perform an assessment each year with the following objectives:

- ✓ To ensure that the risks are being managed in the manner approved by senior management and the management team.
- ✓ To evaluate whether the agreed-upon responses are efficient and to implement action plans if necessary.
- ✓ To determine whether the risk catalogue anticipates and reflects changes in the business circumstances and new economic conditions.

Additionally, the Compliance Department must identify whether any risk has materialised and, where applicable, the measures implemented to mitigate it.

The following reporting levels will exist to facilitate risk monitoring:

- a) **Internal reporting:** The Risk Map Report, which will include the Risk Map and the risk catalogue of CIE Automotive, and a graphic representation of the main risks by geographic area and type of risk, including the high-level control activities implemented for the top risks, as well as the action plans established to mitigate them.
- b) **External reporting:** This is comprised of the information on risk management to be included in the Non-Financial Information Statement, the Annual Corporate Governance Report and in

Issued and reviewed: Audit and Compliance Committee	Approved: Board of Directors	Date: October 2020
--	-------------------------------------	---------------------------

	RISK CONTROL AND MANAGEMENT POLICY	Code:	CIE CO CP PO 03
		Review:	04
		Page:	8 of 8

the Annual Report, in which the main risks to which CIE Automotive is exposed and the actions established in relation to the main risks identified are detailed.

The monitoring of the ESG risks by the Board and the Audit and Compliance Committee meets GRI Standards.

4.5. Updating and monitoring

The business risks change over time and, therefore, give rise to changes in the RMS. In the connection, risks that were critical may lose relevance, while others may gain importance.

To maintain an effective and up-to-date RMS, the Compliance Department updates the Risk Map annually following the process described above.

The Audit and Compliance Committee is responsible for monitoring the RMS.

4.6. Breach

Any employee that has evidence or suspects irregular behaviour or behaviour that could lead to the materialisation of a risk must immediately inform CIE Automotive through the whistle-blowing channel available on the corporate website.