




CIE Automotive

Risk Control and Management Policy

	RISK CONTROL AND MANAGEMENT POLICY	Code:	CIE CO CP PO 03
		Version:	05
		Page:	2 of 10

Contents

1. Purpose	3
2. Scope of application.....	4
3. Responsibilities	4
4. Description of the process	5
4.1. Risk identification.....	6
4.2. Risk assessment	7
4.3. Risk handling	8
4.4. Action plans.....	9
4.5. Risk oversight	9
4.6. Updating and monitoring.....	10
4.7. Non-compliance	10
5. Terms and definitions	10
6. Approval of the policy	10

	RISK CONTROL AND MANAGEMENT POLICY	Code:	CIE CO CP PO 03
		Version:	05
		Page:	3 of 10

1. Purpose

The purpose of this document is to define the Risk Control and Management Policy (the “**Policy**”) for CIE Automotive, S.A. and its subsidiaries¹ (“**CIE Automotive**”, the “**Group**” or the “**Company**”), in order to establish the general framework of activities, procedures, and responsibilities used to ensure effective and efficient control and management of the risks that could affect CIE Automotive.

CIE Automotive’s risk management system (“**RMS**”) provides reasonable certainty that all significant financial and non-financial risks are being prevented, identified, assessed, continually monitored, and reduced to levels that comply with the risk tolerance levels defined, with final approval by the Board of Directors (“**Board**”).

CIE Automotive classifies the risks into the following categories: strategic, operational, financial, compliance, and ESG (Environmental, Social, and Governance).

With a strong and sustained commitment from Senior Management and the Management Team, along with rigorous strategic planning, the overall aim is to achieve an environment where risks can be addressed in a controlled manner and actively managed, making it possible to take advantage of new opportunities.

The RMS is based on the following fundamental principles:

- ✓ Promoting a productive vision of the concept of risk.
- ✓ Ensuring the commitment and competence of all participants.
- ✓ Promoting use of a common language.
- ✓ Achieving transparent communication throughout the entire Group.
- ✓ Integrity: the Company must establish an RMS that allows all significant risks that could affect the Group to be identified and kept within defined tolerance limits, with the aim of ensuring business continuity and achievement of the Group’s planned objectives.
- ✓ Monitoring: the Company must perform oversight to ensure adequate identification, measurement, assessment, and control of all significant risks that could affect the Group.
- ✓ Proactivity: the Company must promote a proactive system of risk management that helps mitigate the risks, including implementation of contingency and hedging plans whenever possible.

All of CIE Automotive’s personnel with responsibilities related to the RMS must have the material and human resources necessary to perform their functions.


In this Policy, CIE Automotive defines the guidelines to be followed for identifying the risks and keeping them within the tolerance limits approved by the Board at any given time.

The procedures implemented via this Policy must be consistent with the principles and guidelines established here in relation to:

- ✓ Contributing to achievement of the Company’s strategic objectives.
- ✓ Introducing the strongest possible safeguards for protecting the corporate interest, and therefore the interests of the shareholders and other stakeholders.
- ✓ Protecting CIE Automotive’s reputation.
- ✓ Safeguarding the ongoing stability of CIE Automotive’s business activities and financial solvency.
- ✓ Contributing to compliance with all legal requirements, as well as all commitments the organisation has taken on voluntarily.
- ✓ Facilitating performance of the operations in compliance with the agreed security and quality standards.

¹ With the subsidiaries being the companies where CIE Automotive, S.A. directly or indirectly owns more than 50% of the share capital and/or has appointed more than half the members of the management body.

Issued and reviewed: Audit and Compliance Committee	Approved: Board of Directors	Date: February 2024
--	-------------------------------------	----------------------------

	RISK CONTROL AND MANAGEMENT POLICY	Code:	CIE CO CP PO 03
		Version:	05
		Page:	4 of 10

In accordance with the above, this Policy is based on the following fundamental principles:

- ✓ Promoting a risk-based focus, with reasonable proportionality and security in view of the existing context, and from the time when the strategy is defined until those variables are incorporated into the operational decisions.
- ✓ Separating the risk-affected areas and assigning responsibilities to them, and to those in charge of risk analysis, control, and oversight, while also ensuring use of the most effective instruments for risk hedging.
- ✓ Transparent reporting on the Group's risks and functioning of the control systems, via the approved communication channels.
- ✓ Ensuring compliance with the corporate governance rules, with updating of those rules in accordance with international best practices on the subject, while also complying at all times with the corporate governance legislation and standards that apply to the Company.

2. Scope of application

This policy applies to CIE Automotive's RMS as implemented at all of its work centres and subsidiaries, under all applicable scopes, and it covers all risks that affect or could affect CIE Automotive, whether derived from its work environment or from its activities. Those risks are classified using the categories defined in section 4.1.

3. Responsibilities

The persons with responsibility for implementing this policy are CIE Automotive's Board members, Senior Management, Management Team, and employees, all within their scope of management, and in each case, they must coordinate their risk-response actions with any other management bodies and departments affected.

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

Body	Responsibilities
Board of Directors <i>(via the ACC)</i>	<ul style="list-style-type: none"> ✓ Highest level of responsibility to the stakeholders for the existence and functioning of the RMS. ✓ Ensuring the existence and suitable design of the RMS. ✓ Overseeing the RMS via the activities performed by the ACC.
Compliance Body	<ul style="list-style-type: none"> ✓ Responsible for designing and implementing the RMS, and for its functioning. ✓ Defining CIE Automotive's methodology, procedures, and criteria for identifying, assessing, classifying, approving, and responding to the risks. ✓ Responsible for producing the Risk Map. ✓ Design the controls for preventing or mitigating the risks identified, and monitor the performance of those controls ✓ Periodic reporting to the ACC regarding evolution of the risks and overall functioning of the RMS.
Internal Audit Department	<ul style="list-style-type: none"> ✓ Assessing the effectiveness of the RMS and reporting periodically to the ACC, Senior Management, and Management Team, regarding any weaknesses detected and scheduling of the proposed corrective measures, as well as proposing recommendations for their improvement.

Issued and reviewed: Audit and Compliance Committee	Approved: Board of Directors	Date: February 2024
--	-------------------------------------	----------------------------

Senior Management and Management Team	<ul style="list-style-type: none"> ✓ Responsible for identifying and assessing the risk. ✓ Ensuring implementation and conveyance of a risk-focused culture at the company. ✓ Defining, establishing and/or modifying the risk tolerance level, which must be sent to the Board for its approval. ✓ Approving the plans and actions proposed by the Compliance Body that could be considered necessary for addressing the identified risks. ✓ Performing a dynamic self-assessment process, which contains information about compliance with the existing policies, procedures, and controls, and about the risks derived from their daily activities. ✓ Perform annual reporting to the Compliance Body regarding evolution of the risks, the preventive measures implemented, and any additional measures proposed.
Other personnel from the Group	<ul style="list-style-type: none"> ✓ Persons responsible for identifying risks that threaten compliance with their objectives, and reporting these to the person responsible from the area. ✓ Collaborating with the persons responsible from the area during risk assessment and classification; proposing action plans to handle the identified risks; and collaborating during execution of those plans.

Table showing the separation of functions for the RMS:

	Board of Directors	Compliance Body	Internal Audit Department	Senior Management and Management Team	Other personnel from the Group
Risk identification		X		X	X
Risk assessment		X		X	
Risk handling		X			
Risk oversight	X	X	X		
Updating		X		X	
Non-compliances			X		X

4. Description of the process


CIE Automotive establishes an RMS for the entire Group, based on the principles described above. That system must use suitable tools to identify the main risks that could affect the Group, assess the probability of occurrence of those risks and their potential impacts on the financial statements and on the Group's business, and assess the control measures necessary to mitigate them. In particular, the Company has a Risk Map, which it must periodically update and review (at least on an annual basis).

The purpose of this RMS is not to eliminate all risks that could affect the Group, but instead, to establish a tolerance level that allows generation of value in a recurring and sustainable way. Any risks that are outside of the tolerance levels established must be managed in order to bring them back to the desirable levels, provided the cost of the corresponding mitigation measures is justified by the impact that materialisation of the risk could have on the Group.

CIE Automotive defines a risk as any event, whether caused by internal or external factors, that hinders or prevents achievement of its strategic or operational objectives.

The RMS implemented by CIE Automotive is comprehensive and covers all significant risks, of any nature, that CIE Automotive could be exposed to, especially those that could affect compliance with the Strategic Plan.

The RMS is based on the ISO 31000 methodology, and is adapted to CIE Automotive's needs. The SAP GRC risk management tool is used to support the RMS, with the following main components being defined in it:

	RISK CONTROL AND MANAGEMENT POLICY	Code:	CIE CO CP PO 03
		Version:	05
		Page:	6 of 10

4.1. Risk identification

The risk identification process consists of searching for events (associated with internal or external factors) that could affect CIE Automotive's objectives from the Strategic Plan (a combination of business and sustainability) or the annual budgeting.

That identification includes analysis of:

- ✓ Events that could affect (create or prevent, improve or worsen, accelerate or delay) achievement of the objectives.
- ✓ The sources of risk, including those that are under the Company's control and those that are not.
- ✓ The areas of the Company or project where the risks could have an impact.
- ✓ The causes and potential consequences, the cumulative or domino effects, and the risk scenarios.
- ✓ The locations where the risks originate.
- ✓ Identifying those with responsibility for managing the risks.

The identification process should be performed in various sessions:

- ✓ Prior to initiation of new operations, processes, or activities.
- ✓ Periodically (at least half-yearly).
- ✓ On an ad hoc basis (whenever relevant changes are detected).

The following risk categories are defined:

- ✓ **Strategic:** risks that affect high-level objectives directly related to the Strategic Plan.
- ✓ **Operational:** risks that affect the objectives linked to effective and efficient use of resources.
- ✓ **Financial:** risks that affect the financial objectives.
- ✓ **Compliance:** risks related to infringements by Senior Management or the employees of external legislation or standards, or internal rules.²
- ✓ **Environmental, Social, and Governance (ESG):** these risks affect environmental, social, ethical, and corporate governance aspects, or compliance with laws or standards.

It is important to understand the **external factors**, to ensure that the objectives and concerns of the stakeholders 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 existing at the international, national, regional, or local level.
- b) The factors and trends that could have an impact on the organisation's objectives.
- c) Stakeholder relations.

The **internal factors** are those that the organisation is able to influence, and therefore manage the risk. The risk management process must be consistent with the organisation's culture, processes, structure, and strategy.

A list of risks is compiled as a result of the risk identification process, with the following information included:

- ✓ The risk coding (ID)
- ✓ Each risk's effect (threat or opportunity) and type (strategic, financial, operational, ESG, or compliance)
- ✓ A description or definition of the risk
- ✓ The objective affected by the risk

² Compliance risk management must be performed by taking into account the criteria and guidelines established in the Compliance Management System Manual.

	RISK CONTROL AND MANAGEMENT POLICY	Code:	CIE CO CP PO 03
		Version:	05
		Page:	7 of 10

4.2. Risk assessment

Risk assessment is the process of comparing the level of risk with the established risk criteria, so that decisions can be made about how to prioritise and handle each risk.

Assessment scales have been defined for probability of occurrence and impact, to create a standardised way of assessing the risks.

$$\text{Risk Level (R)} = \text{Probability of occurrence (P)} \times \text{Impact (I)}$$

The following general Probability of occurrence (P) values are established:

5 - Very high	4 - High	3 - Moderate	2 - Low	1 - Very Low
> 80%	61% - 80%	31% - 60%	10% - 30%	< 10%
The risk has materialised more than 5 times in the last 2 years.	The risk has materialised more than 5 times in the last 5 years.	The risk has materialised more than 5 times in the last 10 years.	The risk has materialised 1 to 4 times in the last 10 years.	The risk has not materialised, or materialised more than 10 years ago.
If the risk materialises it will affect the organisation immediately (during the current financial year).	If the risk materialises it will affect the organisation within one year (the following financial year).	If the risk materialises it will affect the organisation within the next two years.	If the risk materialises it will affect the organisation within the next five years.	If the risk materialises it will only affect the organisation after more than five years.

Probability of occurrence for climate change risks:

5 - Very high	4 - High	3 - Moderate	2 - Low	1 - Very Low
> 80%	61% - 80%	31% - 60%	10% - 30%	< 10%
If the risk materialises it will affect the organisation soon (within the next three years).	If the risk materialises it will affect the organisation before the year 2030.	If the risk materialises it will affect the organisation between the years 2030 and 2040.	If the risk materialises it will affect the organisation within 20 years after the year 2040.	If the risk materialises it will not affect the organisation until after the year 2050.

The (P) value must be based on the best possible estimate, using the information available.

The Impact (I) values are established in relation to three categories: financial, organisational, and reputational. These scales are used to position each risk on the Risk Map, which is the primary risk assessment tool.

5 - Very high	4 - High	3 - Moderate	2 - Low	1 - Very Low
EBITDA would decrease very sharply. Generates a negative impact on the P&L of more than 5%.	EBITDA would decrease sharply. Generates a negative impact on the P&L of more than 3.5%, up to 5%.	EBITDA forecasts would decrease significantly. Generates a negative impact on the P&L of more than 1.5%, up to 3.5%.	EBITDA forecasts would decrease slightly. Generates a negative impact on the P&L of more than 0%, up to 1.5%.	The current EBITDA level would be maintained.
Organisational impact				
If the risk materialises the Board would have to become involved.	If the risk materialises the CEO would have to become involved.	If the risk materialises it could be resolved at the corporate level.	If the risk materialises it could be resolved at the level of each division.	If the risk materialises it could be resolved at the level of each facility.
Reputational impact				
Loss of reputation by various activities that have a severe effect on the image and share price.	Loss of reputation by various activities that have an effect on the image and share price.	Occurrence of an event that is reported in major media sources and becomes known to the regulator/analysts.	Occurrence of an event that is reported in local media sources.	No impact.


¹ Profit & Loss account.

The event will generate either a negative risk (threat) or positive risk (opportunity), depending on whether its impact on the Group is negative or positive.

Also, when the risks are being assessed based on their type, the speed of occurrence may also be considered, which is defined as the amount of time that passes from materialisation of the risk until that risk directly or indirectly affects CIE Automotive's objectives.

The Compliance Body is responsible for the risk assessment process, and it must assess the risks identified within the time periods established.

Issued and reviewed: Audit and Compliance Committee	Approved: Board of Directors	Date: February 2024
--	-------------------------------------	----------------------------

	RISK CONTROL AND MANAGEMENT POLICY	Code:	CIE CO CP PO 03
		Version:	05
		Page:	8 of 10

Once the risk assessments are completed, they must be consolidated in order to produce the Risk Map, where the risk levels are represented as a table of probabilities of occurrence and impacts, using the following risk criteria:

Risk Level	Risk Decision ³
High or Very High	The assessed risk (threat/opportunity) is considered unacceptable. It must be actively handled and controls must be established.
Moderate	The assessed risk (threat/opportunity) is considered potentially unacceptable. That way it must be handled depends on the context, but controls must be established.
Low or Very Low	The assessed risk (threat/opportunity) is considered acceptable. That way it must be handled depends on the context, but controls do not have to be established.

The Compliance Body performs consolidation of the risks, taking into account the specific weights of the assessments performed by each of the persons responsible and each geographic area, for each type of risk. This results in a global vision for CIE Automotive, and allows the risks to be prioritised.

4.3. Risk handling

Once the risks have been identified, assessed, and consolidated, action plans must be prepared to ensure that the organisation's accepted risk level will not be exceeded.

Strategies for handling negative risks (threats):

- ✓ **Mitigate:** These are actions designed to reduce a risk's probability of occurrence or impact, to the level acceptable for the organisation.
- ✓ **Accept:** The risk's probability of occurrence and consequences are considered acceptable, so no actions are taken for that risk.
- ✓ **Share:** Actions are taken so that some of the risk will be shared with external parties, such as by taking out insurance, outsourcing processes, etc.
- ✓ **Avoid:** The activity generating the risk is suspended in order to eliminate the risk. This strategy eliminates the threat or provides full protection against its impact.


Strategies for handling positive risks (opportunities):

- ✓ **Take advantage:** Measures are implemented to take advantage of an opportunity and make sure it will occur.
- ✓ **Increase:** Actions are taken in order to increase an opportunity's probability of occurrence or positive impact.
- ✓ **Share:** Actions are taken to fully or partially transfer ownership of an opportunity to an external party that is better able to take advantage of it.
- ✓ **Accept:** The opportunity is recognised but it is not actively pursued, i.e., it will be taken advantage of if it materialises.

The options for handling each risk are selected based on the specific needs and circumstances of the organisation or project. It is essential to periodically review the options selected, to ensure that the residual risk levels are still within the risk tolerance limits. These ongoing reviews also allow assessment of the effectiveness of the measures implemented, and new ways of handling the risks can also be implemented, if necessary, in order to effectively mitigate or manage the risks.

For each of the risks identified, especially the critical risks, periodic monitoring must be performed and its potential materialisation must be analysed, using suitable quantitative or qualitative indicators. In any cases

³ The Compliance Body has final decision-making authority regarding the need to handle a risk or establish controls for it.

	RISK CONTROL AND MANAGEMENT POLICY	Code:	CIE CO CP PO 03
		Version:	05
		Page:	9 of 10

where an indicator exceeds the established tolerance, the causes must be identified and action plans or responses must be proposed by the identified persons responsible.

4.4. Action plans

Specific action plans are developed based on the risk handling process, and they must cover the following aspects:

- ✓ Reasons supporting the decision to implement the risk handling option selected.
- ✓ Objectives to be achieved with the risk handling plan.
- ✓ Persons responsible for approving and implementing the action plan developed for the risk.
- ✓ Proposed actions and tasks, with specification of the resources needed.
- ✓ Current status of the plan, along with the control and monitoring mechanisms.
- ✓ Information that should be communicated to the parties or stakeholders affected.
- ✓ Residual risks still remaining after the risk handling.
- ✓ Any other pertinent observations or comments.

4.5. Risk oversight

With the objective of ensuring that the agreed responses to the risks are still viable and effective, the Compliance Body must perform monitoring each year, which must cover the following objectives:


- ✓ Ensuring that the risks are being managed in the way that Senior Management and the Management Team have approved.
- ✓ Assessing the agreed responses to determine whether they are effective, and initiating the action plans in cases where necessary.
- ✓ Determining whether the risk catalogue is anticipating and reflecting changes to the business circumstances, new economic conditions, and any other new conditions.

In addition, the Compliance Body must determine whether any risks have materialised, and for any that have, it must identify the measures implemented to mitigate them.

There must be different levels of reporting to facilitate the oversight work:

- a) **Internal reporting:** which includes CIE Automotive's **Risk Map** and risk catalogue, plus a graphic representation of the main risks by geographic area and by risk type, also including the high-level control activities implemented for the top risks.
The persons responsible for the risks associated with all areas, assets, and projects must report their main threats and opportunities to the Compliance Body (which is in charge of oversight of the model) if they require decisions from that body (at least those associated with a "High or Very High" risk level). The Compliance Body must compile and integrate all of the information, producing a Risk Map that will allow:
 - Monitoring of the risk portfolio in an integrated manner
 - Unification of the handling actions or controls (where applicable)
 - Preparation of internal or external reports
- b) **External reporting:** this means the reporting on risk management that will be included in the Non-Financial Information Statement, Annual Corporate Governance Report, Management Report, Annual Report, and Notes to the Consolidated and Standalone Annual Accounts, and the reporting that will be included in any other reports that may come to replace any of those listed above, or any that is required in accordance with the legislation or standards that apply at any given time. That external reporting must include details of the main risks affecting CIE Automotive, and the actions agreed with regard to the main risks identified.

Issued and reviewed: Audit and Compliance Committee	Approved: Board of Directors	Date: February 2024
--	-------------------------------------	----------------------------

	RISK CONTROL AND MANAGEMENT POLICY	Code:	CIE CO CP PO 03
		Version:	05
		Page:	10 of 10

4.6. Updating and monitoring

The business risks change over time, and this generates changes in the RMS. For example, risks previously classified as critical may have lost relevance, while others may have become more critical.

To ensure that the RMS remains effective and up-to-date, the Compliance Body performs an annual updating of the Risk Map, following the process described above.

4.7. Non-compliance

Any employee who suspects or has evidence of improper conduct and/or conduct that could involve materialisation of a risk must immediately notify CIE Automotive via the Ethical Channel, which is made available at the corporate website.

5. Terms and definitions

- For purposes of this document, the following terms and definitions will apply:
- Employees: Members of the Board and all of CIE Automotive’s personnel and collaborators, regardless of the type of relationship or contract they have.
- Risk Management System (RMS): an organisation’s set of interrelated or interacting elements, subject to final approval by the Board of Directors, that provide reasonable assurance that all risks included in the defined categories are being prevented, identified, assessed, subjected to ongoing monitoring, and reduced to levels that comply with the defined risk tolerance levels.
- Compliance Management System (CMS): an organisation’s set of interrelated or interacting elements used to establish policies and objectives, along with the processes used to achieve those objectives.
- Compliance Body: persons from the Compliance Department with responsibility and authority for operation of the CMS.
- Compliance: means compliance with all of the organisation’s obligations relating to compliance.
- Compliance objectives: development of the compliance culture for internal rules and external laws and standards, and commitments relating to criminal law, including but not limited to those regarding prevention of criminal offences and bribery, environmental protection, and taxation.
- Compliance risk: the probability of occurrence and consequences of failure to comply with an organisation’s compliance obligations.

The compliance risks for Senior Management, or for other people within the organisation, must be understood as including, among others:

- Risk of non-compliance with the ethical principles and internal rules, by the employees or by the Group itself, and including new business operations and geographic areas.
- Risk of legal non-compliances, contractual breaches, or improper professional practices (for example, misinterpretation of a specific regulation).
- Reputational risk.
- Operational risks derived from the cases described above.

6. Approval of the policy

This policy was approved by the Board and entered into force on that same date. It may only be modified by means of a new resolution expressly passed by that management body, which will be responsible for the necessary distribution.

Issued and reviewed: Audit and Compliance Committee	Approved: Board of Directors	Date: February 2024
--	-------------------------------------	----------------------------