

# **ENTERPRISE RISK MANAGEMENT POLICY**

**Approved by the Board of Directors**

**on August 9, 2018 and revised on April 26, 2022**

## **1. OBJECTIVE**

This policy aims to establish guidelines for Embraer's risk management process to ensure that the identification, analysis, assessment, mitigation, and monitoring of risks are conducted in accordance with the methodology defined by the Senior Management, considering the Company's strategic planning, processes, business model and external factors. Additionally, the communication of the Enterprise Risk Management policy aims to raise awareness and continuously train employees for the dissemination of the risk culture.

## **2. SCOPE AND APPLICATION**

The Enterprise Risk Management Policy covers Embraer S.A and its controlled companies. Integrated Risk Management is applied to the Presidency, Vice-Presidencies, directors, and managers, as well as areas of the Company that seek support in the conduction of their processes, to manage the exposure of their internal or external risks, inherent to Embraer's business, in order to ensure that they are properly documented, monitored and treated.

The Company has specific policies to deal with the risks of financial operations and the unfolding of events whose consequences may jeopardize the continuity of operations.

## **3. DEFINITIONS**

**Action Plan (PA):** corporate document that consolidates a short-term vision of the Company's intended goals and results.

**Audit, Risk and Ethics Committee (CARE):** board without deliberative or management power, intended to assist the Board of Directors in the exercise of its functions, focusing on monitoring the risk assessment, management and accounting information and Compliance. The Committee also functions as an Audit Committee for the purposes of US law and as a Statutory Audit Committee.

**Board of Directors (CA):** collegiate decision-making body whose attributions and powers are provided for in Embraer's Bylaws and in the law.

**Company:** refers to the offices and sites of Embraer S.A. (Brazil and abroad) and its Subsidiaries.

**Impact:** result or effect of a risk. There are several possible impacts associated with a risk. The impact of a risk adversely affects the Company's strategy or business objectives.

**Inherent Risk:** risk to the Company in the absence of any direct or directed actions by management to reduce its severity.

**Key Performance Indicator (KPI):** quantitative or qualitative measures that demonstrate progress towards an intended outcome and assist in tracking existing action plans.

**Key Risk Indicator (KRI):** quantitative or qualitative measures that help identify changes in existing risks.

**Policy:** a set of Company guidelines in relation to a relevant topic, applicable to Embraer and its subsidiaries that have employees. The Policy guides actions at all levels of the Company.

**Process Owner:** responsible for certain business processes within the Company.

**Residual Risk:** the risk remaining after Management addresses the measures to reduce its exposure to the Embraer business environment.

**Risk:** defined in COSO ERM (Enterprise Risk Management), it is the possibility of occurrence of an event, originated from internal or external sources, capable of affecting the achievement of the Company's Strategy and business objectives.

**Risk Appetite:** refers to the level of risk that the organization can accept, as established for its vision and mission, indicating the degree of acceptable exposure in its quest to create and maintain value.

**Risk Factor:** causes that may lead to the materialization of a risk.

**Risk Management:** defined as the culture, capabilities, and practices, integrated with the establishment of strategies and performance, on which organizations rely to manage risks in the creation, preservation, and realization of value. As one of the main references of an integrated Risk Management structure, Embraer seeks to follow the guidelines established by the COSO ERM (Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management) version 2017.

**Risk Owner:** responsible for the risks in the area and their respective management.

**Risks Portfolio:** a list of risks that the Company is subject to in the execution of its operations. It is structured by categories to provide standard definitions for different risks allowing similar risks to be grouped together. Also, within each category, risks are defined in more detailed subcategories.

**Risk Tolerance:** Acceptable variation around the established limits for the risks accepted by the Company.

**Stakeholder:** person or group that legitimizes the Company's actions and can affect or be affected by its management and results.

**Strategic Plan (PE):** corporate document that consolidates a medium and long-term visions of the strategies and results intended by the Company.

**Vulnerability:** the level of risk exposure considering the Company's current control structure: future perception, efficiency and effectiveness of controls, history, and previous risk impacts.

#### 4. GUIDELINES

The guidelines presented here define and characterize the macro stages of the Company's Enterprise Risk Management process aimed at:

- Strengthening the Enterprise Risk Management Culture.
- Ensuring that Governance principles are followed.
- Standardizing concepts and practices.
- Defining roles and responsibilities.
- Supporting the execution of the strategy and the achievement of Embraer's business objectives.
- Ensuring the most adequate response to risks.
- Ensuring proper prioritization/analysis, assessment, and monitoring of risks.
- Ensuring proper risk reassessment based on performance and current scenario, as well as proper risk reporting and communication.



*Image 01 - COSO ERM 2017 - Components of Risk Management*

#### **4.1 Governance and Culture**

The Board of Directors and the Audit, Risks and Ethics Committee monitor and supervise the existing risks to Embraer's business. Both forums have members with extensive experience and knowledge about the Company and the Risks subject.

The Company has a corporate governance structure, whose Compliance, Risks and Audit areas are aligned and act as second and third lines, ensuring their reporting structures and directing employees regarding the expected behaviors and culture to meet the established mission, vision, and values.

Management trains its employees in charge of Enterprise risk management and provides training for the various areas that contribute to the process, including CARE's leaders and members.

The Risk management process and this Policy are periodically reviewed based on benchmarking, updates in frameworks and best market practices.

#### **4.2 Strategy and Goal Setting**

Annually, the Board of Directors and the Executive Board of Embraer S.A. review the goals (short and medium terms) and strategic objectives (long term) of the Company. Additionally, there is a periodic alignment between the governance areas to identify relevant subjects, existing or emerging, to be considered in the Enterprise Risk Management process.

Finally, considering the expected results, business specifics, influences from the internal (capital, people, processes, performance, and technology) and external (political, economic, social, technological, legal, and environmental) environments, in addition to risk appetite, the context of Enterprise Risk Management is defined.

##### **• Risk Appetite Statement**

Risk appetite levels are suggested by the Risk management department, reviewed by the Audit, Risks and Ethics Committee and defined by the Board of Directors (CA), during the review of the

Strategic Plan, based on the degree of uncertainty that Embraer is willing to assume to achieve its goals and business plan.

### 4.3 Performance

The Risk Management area, alongside with the business areas, analyzes the sources of risks, affected areas, causes and potential consequences that may affect Embraer's strategic goals and/or objectives.

Enterprise risks related to the Company's strategic objectives and the internal and external environments (Context) are identified and prioritized to ensure that any materializations that may occur are known in advance and managed to an acceptable level. The identification and reassessment of risks take place both through a top-down approach (analyses with executives) and a bottom-up approach (indicators, process analyses, questionnaires directed to management).

Enterprise risks can be classified into the following categories:

- **Strategic:** risk associated with strategic decisions made by senior management aimed at achieving its business objectives, ensuring the Company's ability to protect itself or adapt to changes in the environment in which it operates.
- **Financial:** risk that may affect the Company's financial operations, as well as the reliability of reports.
- **Regulatory:** risk of legal or regulatory sanctions, financial or reputational loss that Embraer may suffer because of failure to comply with the application of laws, agreements, regulations, the Code of Ethics and Conduct, among others.
- **Operational:** refers to possible losses of efficiency and effectiveness on the Company's operations.
- **Cybernetic:** risk associated with systems security in terms of confidentiality, integrity and availability of data and information.

After analyzing each risk, they are evaluated using impact and vulnerability criteria for prioritization in the heat map. Based on the results, each business area defines the treatment to be given to the risk.

### 4.4 Analysis and Review

For Enterprise risk management to be effective, Risk Owners and Process Owners monitor the identified and prioritized risks based on the evolution of KRIs and KPIs and on the best Risk Management practices established by Embraer.

Likewise, periodic analyzes are carried out with the Vice-Presidents, directors, and managers to review the prioritized risks, their assessments and response plans, as well as identify new risks. Finally, risk management is reviewed whenever necessary based on a Strategy update, changes in risk appetite and/or changes in the business context.

#### **4.5 Information, Communication and Disclosure**

The risks are consolidated in a specific management tool. The Risk Management area reports Enterprise risks to the CFO, CEO and to CARE and CA.

Additionally, the main risks inherent to the Company's business are disclosed to the market through annual reports 20-F and the Reference Form.

### **5. ROLES AND RESPONSIBILITIES**

#### **5.1 Risk Management:**

- Coordinate and define standards related to integrated risk management processes.
- Support and ensure the identification, reporting and monitoring of risks and their respective action plans.
- Carry out the consolidation of risks.
- Periodically and formally report to CARE, CA and at Executive Board Meetings (RD), when requested.
- Disseminate the risk management culture in the Company.

#### **5.2 Executive Boards:**

- Lead the implementation of risk management in their respective areas.
- Approve norms, maximum limits of specific risks in their respective areas, if necessary.
- Manage the risks inherent to its activities (identify, assess, treat and monitor).
- Define and monitor action/mitigation plans to reduce exposure to risk, as well as define those responsible, indicators and action implementation deadlines (when applicable).
- Inform the Risk Management area about the identification of new risks or events that are relevant and their respective evolutions.

### **5.3 CEO and CFO:**

- Exercise leadership and direction to the administration through the definition of objectives, fundamental values, standards, expectations, organizational structure, and responsibilities of the Company.
- Approve key documents (e.g., Enterprise Risk Management policy).
- Monitor prioritized risks periodically.
- Evaluate reports and results and provide appropriate considerations and guidance.

### **5.4 Audit, Risk and Ethics Committee:**

- Supervise and suggest revisions on the most relevant risks of an operational, strategic, financial, regulatory, or cybernetic nature in the markets managed by the Company, by diagnosing the sources of risk in Embraer's activities and its strategy.
- Assess the adequacy of risk management and assessment models, as well as adequacy of adherence tests and validation of the models used.
- Analyze and give an opinion on Enterprise risk management guidelines and policies, especially about risk appetite and risk culture.
- Analyze and give an opinion on the managerial and accounting information disclosed to the public and regulatory bodies regarding the Company's risk profile and control.
- Assess the adequacy of human and financial resources for risk management.
- Exercise the functions of (i) Audit Committee for the purposes of North American legislation, especially the “Sarbanes-Oxley Act”, and of (ii) Statutory Audit Committee, pursuant to Instruction 509, of November 16, 2011 (“CVM Instruction 509”), from the Brazilian Securities and Exchange Commission (“CVM”).

### **5.5 Board of Directors:**

- Review and deliberate on the Enterprise Risk Management Policy.
- Supervise and monitor the risks that Embraer is exposed to, whether of a financial, strategic, regulatory, operational, or cybernetic nature.

## **6. GENERAL PROVISIONS**

It is the responsibility of the business areas to communicate any changes in the Risk Management process to the Risk Management team for treatment and approval by the Board.

The operational procedures and activities of the Risk Management process are described in the risk management procedure.

This policy must be reviewed, minimally, every two years.