

<b>BONFIGLIOLI TRANSMISSIONS LIMITED</b>	<b>Version No.</b>	01
<b>CIN: U29309TN1998PLC040717</b>	<b>Prepared by</b>	Secretarial Department
<b>Registered Office:</b> Plot No. AC7-AC11, SIDCO Industrial Estate, Thirumudivakkam, Kancheepuram, Tamil Nadu, India, 600 132	<b>Effective date</b>	February 5, 2026
	<b>Last Amendment on</b>	-

## RISK MANAGEMENT POLICY

### 1. Background

Section 134(3) of the Companies Act, 2013 requires a statement to be included in the report of the board of directors (“**Board**”) of Bonfiglioli Transmissions Limited (“the “**Company**”), indicating development and implementation of a risk management policy for the Company, including identification therein of elements of risk, if any, which, in the opinion of the Board, may threaten the existence of the Company.

Furthermore, Regulation 17(9) of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015, as amended (“**SEBI Listing Regulations**”), requires that the Company set out procedures to inform the Board of risk assessment and minimization procedures and makes the Board responsible for framing, implementing and monitoring the risk management plan of the Company.

**Risk:** Risk is an event which can prevent, hinder or fail to further or otherwise obstruct the enterprise in achieving its objectives. A business risk is the threat that an event or action will adversely affect an enterprise’s ability to maximize stakeholder value and to achieve its business objectives. Risk can cause financial disadvantage, for example, additional costs or loss of funds or assets. It can result in damage, loss of value and /or loss of an opportunity to enhance the enterprise operations or activities. Risk is the product of probability of occurrence of an event and the financial impact of such occurrence to an enterprise.

### 2. Objective and Purpose

In line with the Company’s objective towards increasing stakeholder value, a risk management policy has been framed, which attempts to identify the key events / risks impacting the business objectives of the Company and attempts to develop risk policies and strategies to ensure timely evaluation, reporting and monitoring of key business risks.

### 3. Policy

Our risk management approach is composed primarily of three components:

- a) Risk governance
- b) Risk identification
- c) Risk assessment and control

a. Risk governance:

- i. The functional heads of the Company are responsible for managing risk on various parameters and ensure implementation of appropriate risk mitigation measures.
- ii. The risk management committee of the Company (“**Risk Management Committee**”) provides oversight and reviews the risk management policy from time to time.

b. Risk identification:

External and internal risk factors that must be managed are identified in the context of business objectives. In particular, internal risks include financial, strategic, environment, personnel, regulatory, information, cyber security, operational, and external risks include political, sectoral, sustainability (particularly, ESG related risks), or any other risk as may be determined by the Risk Management Committee.

c. Risk assessment and control:

This comprises the following:

- a) Risk assessment and reporting
- b) Risk control
- c) Capability development

On a periodic basis risk, external and internal risk factors are assessed by responsible managers across the organization. The risks are identified and formally reported through mechanisms such as operation reviews and committee meetings. Internal control is exercised through policies and systems to ensure timely availability of information that facilitate pro-active risk management. Examples of certain of these identified risks are as follows:

- i. Broad market trends and other factors beyond the Company’s control significantly reducing demand for its services and harming its business, financial condition and results of operations
- ii. Failure in implementing its current and future strategic plans
- iii. Significant and rapid technological change
- iv. Damage to its reputation
- v. Its products losing market appeal and the Company not being able to expand into new product lines or attracting new types of investors
- vi. Its risk management methods and insurance policies not being effective or adequate
- vii. Fluctuations in trading activities
- viii. Changes in interest rates
- ix. Changes in government policies

- x. Security risks and cyber-attacks
- xi. Insufficient systems capacity and system failures

**4. Risk Scoring:** Management considers qualitative and quantitative methods to evaluate the likelihood and impact of identified risk elements. Likelihood of occurrence of a risk element within a finite time is scored based on polled opinion or from analysis of event logs drawn from the past. Impact is measured based on a risk element’s potential impact on cost, revenue, profit etc. should the risk element materialize. The composite score of impact and likelihood are tabulated in an orderly fashion and the table is known as a ‘Risk Register’. The Company has assigned quantifiable values to each risk element based on the “impact” and “likelihood” of the occurrence of the risk on a scale of 1 to 3 as follows.

Impact	Score	Likelihood
Minor	1	Low
Moderate	2	Medium
Significant	3	High

**5. Risk Categorization:**

The identified risks are further grouped into (a) preventable; (b) strategic; and (c) external categories, to homogenize risks.

Preventable risks are largely internal to the Company and are operational in nature. The endeavour is to reduce /eliminate the events in this category as they are controllable. Standard operating procedures and audit plans are relied upon to monitor and control such internal operational risks that are preventable.

- i. Strategy risks are voluntarily assumed risks by the senior management in order to generate superior returns / market share from its strategy. Approaches to strategy risk is ‘accept’/‘share’, backed by a risk-management system designed to reduce the probability that the assumed risks actually materialize and to improve the Company’s ability to manage or contain the risk events should they occur.
- ii. External risks arise from events beyond organization’s influence or control. They generally arise from natural and political disasters and major macroeconomic shifts. Management regularly endeavours to focus on their identification and impact mitigation through ‘avoid’/‘reduce’ approach that includes measures like business continuity plan / disaster recovery management plan / specific loss insurance / policy advocacy etc.

**6. Risk Prioritization:**

Based on the composite scores, risks are prioritized for mitigation actions and reporting.

## **7. Risk Mitigation**

The following framework shall be used for implementation of risk mitigation:

All identified risks should be mitigated using any of the following risk mitigation plan:

- a) Risk avoidance: By not performing an activity that could carry risk. Avoidance may seem the answer to all risks but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed.
- b) Risk transfer: Mitigation by having another party to accept the risk, either partial or total, typically by contract or by hedging / insurance.
- c) Risk reduction: Employing methods/solutions that reduce the severity of the loss e.g. having adequate software in place to prevent data leak.
- d) Risk retention: Accepting the loss when it occurs. Risk retention is a viable strategy for small Risks where the cost of insuring against the risk would be greater than the total losses sustained. All risks that are not avoided or transferred are retained by default.

## **8. Risk Management Committee**

The Risk Management Committee, which was constituted with the overall responsibility of overseeing and reviewing risk management across the Company. The terms of reference of the Risk Management Committee are as follows:

- (a) to formulate a detailed risk management policy which shall include:  
Review, assess and formulate detailed risk management policy of the company from time to time and recommend for an amendment or modification thereof, which shall include:
  - (i) a framework for identification of internal and external risks specifically faced by the Company, in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the Risk Management Committee;
  - (ii) measures for risk mitigation including systems and processes for internal control of identified risks; and
  - (iii) business continuity plan.
- (b) to ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company;
- (c) to monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems;
- (d) to periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity;
- (e) to keep the Board informed about the nature and content of its discussions, recommendations and actions to be taken;
- (f) the appointment, removal and terms of remuneration of the chief risk officer (if any) shall be subject to review by the Risk Management Committee;

- (g) To coordinate its activities with other committees, in instances where there is any overlap with activities of such committees, as per the framework laid down by the Board; and
- (h) any other similar or other functions as may be laid down by Board from time to time and/or as may be required under applicable law, as and when amended from time to time, including the SEBI Listing Regulations.

## **8. Risk Management Measures adopted in general by the Company:**

The Company has adopted various measures to mitigate the risk arising out of various areas described above, including but not limited to the following:

- i. A well-defined organization structure;
- ii. Defined flow of information to avoid any conflict or communication gap;
- iii. Hierarchical support personnel to avoid work interruption in absence/ non-availability of functional heads;
- iv. Discussion and implementation on financial planning with detailed business plans;
- v. Detailed discussion and analysis of periodic budgets;
- vi. Employees training and development programs;
- vii. Internal control systems to detect, resolve and avoid any frauds;
- viii. Systems for assessment of creditworthiness of existing and potential contractors/subcontractors/ dealers/vendors/ end-users;
- ix. Redressal of grievances by negotiations, conciliation and arbitration; and
- x. Defined recruitment policy.

## **9. Risk Reporting:**

Periodically, key risks are reported to the Board or risk management committee with causes and mitigation actions undertaken/ proposed to be undertaken.

The internal auditor carries out reviews of the various systems of the Company using a risk based audit methodology. The internal auditor is charged with the responsibility for completing the agreed program of independent reviews of the major risk areas and is responsible to the audit committee which reviews the report of the internal auditors on a quarterly basis.

The statutory auditors carries out reviews of the Company's internal control systems to obtain reasonable assurance to state whether an adequate internal financial controls system was maintained and whether such internal financial controls system operated effectively in the company in all material respects with respect to financial reporting.

On regular periodic basis, the Board will, on the advice of the audit committee, receive the certification provided by the chief executive officer and the chief financial officer, on the effectiveness, in all material respects, of the risk management and internal control system in relation to material business risks.

The Board shall include a statement indicating development and implementation of a risk management policy for the Company including identification of elements of risk, if any, which in the opinion of the Board may threaten the existence of the Company.

#### **10. BUSINESS CONTINUITY PLAN (“BCP”)**

The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster. The BCP is generally conceived in advance and involves input from key stakeholders and personnel. BCP involves defining any and all risks that can affect the Company's operations, making it an important part of the organization's risk management strategy.

Risks may include natural disasters- fire, flood, or weather-related events—and cyber-attacks.

- Once the risks are identified, the plan should also include:
- Determining how those risks will affect operations
- Implementing safeguards and procedures to mitigate the risks
- Testing procedures to ensure they work
- Reviewing the process to make sure that it is up to date

#### **11. DISCLAIMER CLAUSE**

The risks outlined above are not exhaustive and are for information purposes only. Management is not an expert in assessment of risk factors, risk mitigation measures and management's perception of risks. Readers are therefore requested to exercise their own judgment in assessing various risks associated with the Company.

#### **12. Amendments and Updatons**

Any change in the Policy shall be approved by the Board or any of its committees (as may be authorized by the board of directors in this regard). The Board of Directors or any of its authorized committees shall have the right to withdraw and / or amend any part of this Policy or the entire Policy, at any time, as it deems fit, or from time to time, and the decision of the Board or its Committee in this respect shall be final and binding. Any subsequent amendment / modification in the SEBI Listing Regulations and / or any other laws in this regard shall automatically apply to this Policy.

#### **13. Communication of the Policy**

This Policy shall be posted on the website of the Company.

\*\*\*\*\*