RISK MANAGEMENT POLICY

OF

SCHNEIDER ELECTRIC INFRASTRUCTURE LIMITED

Version – 3

Effective February 13, 2023
[Pursuant to SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015]

Schneider Electric Infrastructure Limited
Regd. Office: Milestone 87, Vadodara, Halol Highway, Village Kotambi, Post office Jarod, Vadodara GJ 391510 IN
.
CIN: L31900GJ2011PLC064420
Website: www.schneider-infra.in

INDEX

Introduction

Schneider Electric Infrastructure Limited ("the Company") has formulated this Risk Management Policy in line with the provisions of the Companies Act, 2013 ("the Act") and SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("the Listing Regulations").

Risk exists as a consequence of uncertainty and is present in all activities whatever the size or complexity and whatever industry or business sector.

In the current times of stiff competition, where technology is ever evolving and information is available, a business must have a risk management policy to identify and mitigate risks in various aspects of the business.

The Company aims to formulate this risk management policy to be better prepared to deal with risks arising in the course of its operations and to improve the probability of achieving its strategic and operational objectives.

Objective

The objective of the policy is to ensure the commitment towards risk management so as to achieve the strategic and operational goals of the Company.

The policy explains the Company's underlying approach to risk management. It gives key aspects of the risk management process and identifies the main reporting procedures.

Legal Framework

This policy is in compliance with the provisions of Section 134(3)(n) of the Act which requires that the Board annually reports to the shareholders on the implementation of a risk management policy including identification and mitigation of risks relevant to the achievements of the objectives of the Company.
Further, Regulation 9 read with Regulation 21 and Part D of Schedule II of Listing Obligations requires a listed company to have a risk management plan in place, pursuant to which the Board of Directors and Risk Management Committee are responsible to formulate a Risk Management Policy of the Company for identification and monitoring of risks.

Scope of the Policy

This policy is applicable to all operations of the business undertaken by the Company.

Risk Management Strategy

The risk management strategy of the Company, inter alia, includes the following:

1. To identify risks in the operations of the Company, the likelihood and impact and the business owner for the risk;
2. To identify and determine the control improvements to mitigate the risk;
3. To formalise and communicate a consistent approach for managing the identified risks, allocating resources in accordance with the likelihood and impact of the risk;
4. To ensure that a summary of risk identification and mitigation is reported to the Board and Audit Committee;
5. Regular monitoring, review and implementation and effectiveness of the risk management process, including the development of an appropriate risk management culture across the Company.

Internal Control team will facilitate the Risk Assessment process to identify the critical risk and support the management in formulating the risk mitigation plan and monitoring the same.

Constitution of Risk Management Committee

Risk Management Committee ("the Committee") shall be constituted by the Company consisting of such number of directors (executive or non-executive) as the Board may think fit.

The Risk Management Committee shall have minimum three members with majority of them being members of the board of directors, including at least one independent director.

The Chairperson of the Risk management Committee shall be a member of the board of directors.

Senior executives of the listed entity may be members of the committee.

Quorum of the Committee shall be 2 members or 1/3rd of the total members, whichever is higher including at least one member of the board of directors in attendance.

Roles and Responsibilities of Risk Management Committee

The role and responsibilities of the Committee would include the following:

1. The Committee shall function in terms of the terms and reference approved by the Board of Directors of the Company, which forms part of this Policy as Annexure I.

2. Risk management of the Company in accordance with the risk management strategy of the Company;

3. Holding periodical meetings to note emerging risks for consideration and review;

4. Immediately reporting of any significant risk to the Audit Committee of the Company which in turn after discussing the severity of the risk with the Committee shall report the same to the Board of Directors of the Company for taking appropriate action;

5. On receipt of any report from any stake holder of the Company regarding any existing or potential risk, the Committee shall take necessary action as it may deem fit;

6. An annual report may be submitted by the Committee to the Audit Committee, wherein the Committee to present in detail the risk assessed, action taken and the actual and the probable outcomes;

Risk

The Company identifies the following as potential area's of risk on inclusive basis:

- Business risk, sectoral risk, market risk including risk on sales, margins, costs including commodity hedging risk as per framework which form part of this Policy as Annexure II and risks on cash flow;
- Fraud risk, including risk of misreporting;
- Risk of product or service failure;
- Risk relating to safety, health, environment, social and governance;
- Risks related to human resources, including talent retention, gender diversity and sexual harassment;
- Risks related to compliance with laws and regulations;
- Risks related to Business Continuity Plan, including adequacy of disaster management system.

- Risks related to information and cybersecurity

The risk Taxonomy shall form part of the policy as Annexure III.

Amendment

The Company reserves its right to amend or modify this Policy in whole or in part, at any time as considered necessary.

Annexure I

TERMS AND REFERENCE OF RISK MANAGEMENT COMMITTEE

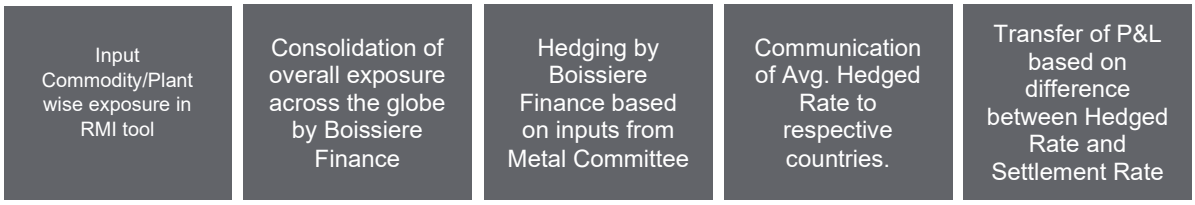
The role of the Risk Management Committee shall, inter alia, include the following:

(1) To formulate a detailed risk management policy which shall include:
(a) A framework for identification of internal and external risks specifically faced by the listed entity, 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 Committee.
(b) Measures for risk mitigation including systems and processes for internal control of identified risks.
(c) Business continuity plan.
(2) To ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company;
(3) To monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems;
(4) To periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity;
(5) To keep the board of directors informed about the nature and content of its discussions, recommendations and actions to be taken;
(6) The appointment, removal and terms of remuneration of the Chief Risk Officer (if any) shall be subject to review by the Risk Management Committee.

The Risk Management Committee shall 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 of directors."

Annexure II

Process Note



- Global Supply Chain team provide the Commodity (5 non-ferrous metals: Copper, Aluminium, Zinc, Nickel and Lead, 1 precious metal: Silver) data quarterly through RMI tool.

- Basis of updating consummation in RMI tool
    - Per unit RM details are populated from Costing sheet (detailed costing with supplier) to get the RM content per unit.
    - Identified RM content used to calculate the yearly consumption based on the year quantity procured.
    - The consumption so arrived at is than declared in the RMI tool based on the eligibility matrix published by global RMI team.
    - The forecasted consumption is declared in the month of RF4 for Y+1 (Aug ~ Sep) and from there on it revised every rolling forecast (Dec/Mar/Jun/Sep) based on the actual data made available.

- This procedure is applicable for transactional business (mainly products) having repetitive commercial flows. For project business, specific request needs to be given with full commodity tonnage volumes for hedging consideration.

- Only manufacturing entities can request hedging for their Raw Materials volumes.
- A hedging agreement is signed by each concerned entity with Boissière Finance.

- For P&L settlement in India, transaction level confirmation would be required in the form [set out in the] underlying documents.

Risk Mitigation Guidelines

The following document defines the policy adopted by the board to hedge the risks arising due to the fluctuations in the prices of Copper, Aluminium, Zinc, Nickel, Lead and Sliver. The policy is organized into the following sections:

A. Identification of Risk
B. Measurement of Risk
C. Hedging of Risk

A. Identification of Risk

As part of its regular business activity, the Company should track the price fluctuations of the various commodities and prepare the exposure which can be defined as contracted and anticipated. Exposure should be reported to Boissière Finance through RMI tool or any other authorized platform.

B. Measurement of Risk

Company would adopt the Global Raw Material Risk Management Policy. Only limited commodities are hedged:

- 5 non-ferrous metals: Copper, Aluminium, Zinc, Nickel and Lead
- 1 precious metal: Silver

C. Hedging of Risk

The Company shall comply with the Global Raw Material Risk Management Policy. *Subject to prior intimation (in writing) to and subsequent ratification by the board of directors of the Company, any changes in Global Raw Material Risk Management Policy shall* be applicable to the Company with immediate effect. Key extracts of Hedging Policy are enclosed herewith:

- A hedging agreement is signed by each concerned entity with Boissière Finance.
- All hedging transactions shall follow rules defined by the Metals Committee aiming at limiting the risks and based a 4 "sliding quarters" process. It means that each quarter as % of hedgeable tonnages is hedged.
- % used for Copper, Aluminium, Zinc, Nickel and Silver (specific process for Lead):
- Minimum by default of 50% to 70 %, 30% to 50%, 15% to 30%, 0 to 15% on the next 4 sliding quarters.
- Maximum of 80% or above subject to Metals Committee decision

Coverage rate

	Minimum	Maximum
Q + 1	50% to 70%	80%
Q + 2	30% to 50%	80%
Q + 3	15% to 30%	80%
Q + 4	0% to 15%	80%

NB: Q= ongoing quarter

Compliance

- Authorised dealer bank ("**AD Bank**") to open a special current account for the company solely for the purpose of commodity settlements. All transactions to be routed through this special current account only.
- The gains/losses proportionate to the company shall be passed by Boissière Finance based on back-to-back agreement along with transaction wise confirmation.
- Annual certificate from the statutory auditors of the entity confirming that the hedge transactions are in line with the exposure of the entity. The statutory auditor shall also comment on the risk management policy of the entity for hedging exposure to commodity price risk and freight risk and the appropriateness of the methodology to arrive at the quantum of these exposures.
- Annual reporting by AD Bank to Chief General Manager, Financial Markets Regulation Department, Reserve Bank of India.

Annexure III

Risk Taxonomy

Risks Category	Risks Type	Risks Category	Risks Type	Risks Category	Risks Type
Environment	Climate Action Failure	Corporate governance	Activist investor's campaign	Tax & customs	Incorrect tax amount paid leading to tax reassessment, penalties or lawsuits
Environment	Bio-Diversity loss	Corporate governance	Capital allocation and value sharing between all stakeholders	Tax & customs	Noncompliance with custom rules leading to business blockage or disruption
Environment	Human Made Environmental Damage	Corporate governance	Lack of oversight by the Board of Director on M&A deals	Customer credit & receivables	Customer Payment default
Environment	Scarcity of resources used in our products or in manufacturing	Corporate governance	Lack of oversight by the Board of Director on risks, compliance and internal control matters and sustainability (especialy climate)	Customer credit & receivables	Late customer payment
Business conduct	Corruption & bribery	Corporate gouvernance	Lack of oversight by the Board of Director on financial statement accuracy and communication	IT systems	Lack of availability of Crown jewels (includes ERP)
Business conduct	Money laundering	Corporate governance	Lack of oversight by the Board of Director on group strategy	IT systems	Lack of availability Financial systems (Includes treasury: payments, receivables, payroll)
Business conduct	Conflict of interest	Liquidity	Lack of liquidity	IT systems	Lack of availability of Connectivity (includes VPN services)
Business conduct	Internal fraud and misappropriation of assets	Accuracy of financial statement	Misstatement of accounts (voluntary or not)	IT systems	Shadow IT (e.g. Kronos)
Business conduct	Internal fraud and misappropriation of assets	Accuracy of financial statement	Lack of timely reporting	IT asset management	IT asset management
Business conduct	Internal fraud and misappropriation of assets	Cybersecurity	Damage to customers assets	IP management	Lack of IP Protection
Business conduct	Fraudulent statement (e.g. to win a deal, financial statement)	Cybersecurity	Damage to customers assets	Data Compliance	Inappropriate Data Privacy
Business conduct	External fraud (eg. fraudulent claim to SE by a customer or partner)	Cybersecurity	Damage to customers assets	Data Compliance	Inappropriate Data Retention
Business conduct	Workplace violations	Cybersecurity	Damage to customers assets	Data Compliance	Inappropriate Data Residency

Business conduct	Workplace violations	Cybersecurity	Business disruption	Data Compliance	Lack of Data Encryption
Business conduct	Workplace violations	Cybersecurity	Business disruption	Data Compliance	Lack of Data Access management and monitoring
Business conduct	Workplace violations	Cybersecurity	Business disruption	Data Compliance	Lack of Data Resilience (back-up and restore)
Business conduct	Workplace violations	Cybersecurity	Business disruption	Data Compliance	Unethical or biased algorithm usage

Risks Category	Risks Type	Risks Category	Risks Type	Risks Category	Risks Type
Business conduct	Workplace violations	Cybersecurity	Compliance	Data Scalability	Lack of authoritative source
Competition law	Non-compliance with competition laws and regulations	Cybersecurity	Compliance	Data Scalability	Lack of common referential
Insider trading & violation of market abuse regulations	Insider dealing	Cybersecurity	Compliance	Data Scalability	Inability to share datasets at scale
Insider trading & violation of market abuse regulations	Targeted employees not part of the blackout periods email list	Cybersecurity	Compliance	M&A and integration	M&A and integration processes
Insider trading & violation of market abuse regulations	Employee not aware of the regulation	Cybersecurity	IP Theft & loss	M&A and integration	Governance of newly acquired companies
Health & Safety	Body cut injuries	Cybersecurity	IP Theft & loss	Anticipation of market evolution	Business models
Health & Safety	Machines	Cybersecurity	IP Theft & loss	Anticipation of market evolution	New competitive landscape
Health & Safety	Driving	Workplace disruption & Security	Site disruption (Short and long term)	Anticipation of market evolution	Technology and new energy landscape
Health & Safety	Falls from heights of people & objects	Workplace disruption & Security	Significant Staff Absence (eg. Pandemic)	Anticipation of market evolution	Sustainability as a business
Health & Safety	Powered Industrial Trucks	Workplace disruption & Security	Business impact in which business contingency plans and capabilities are not adequate	Anticipation of market evolution	Prosumer Innovation at the edge
Health & Safety	Electrical	Workplace disruption & Security	Social & Geopolitical events (e.g. strike, protests)	Global political & economical disruptions	Deglobilization & protectionism
Health & Safety	Ergonomics	Workplace disruption & Security	Theft, sabotage or destruction of company assets or products by external parties	Global political & economical disruptions	Political activism vs business decision

Health & Safety	Handling & Transportation	Workplace disruption & Security	People security (incl sites, travel, WFH)	Global policitical & economical disruptions	Economic cycles
Health & Safety	Fire at a SE location & Flammable material	Product, Project, System quality & Offer reliability	Design Quality and Reliability	New digital offers	Digital customer experience
Health & Safety	Equipment damage at customer worksite	Product, Project, System quality & Offer reliability	Manufacturing Quality and Reliability	New digital offers	Value proposition (incl. Cybersecurity)
Human rights	Child labor	Product, Project, System quality & Offer reliability	Software Quality and Reliability	New digital offers	Capex to Opex

Risks Category	Risks Type	Risks Category	Risks Type	Risks Category	Risks Type
Human rights	Modern Slavery including Forced labor	Product, Project, System quality & Offer reliability	Brand Labeling Quality and Reliablity	New digital offers	Connectivity strategy
Human rights	Migrant Workers	Product, Project, System quality & Offer reliability	Supplier, Subcontractor and Parts Quality and Reliability	New digital offers	Advisor fragmentation
Human rights	Social rights	Product, Project, System quality & Offer reliability	Adaptation Center Quality and Reliability	New digital offers	Monetization models
Human rights	Social rights	Product, Project, System quality & Offer reliability	Projects Execution Quality and Reliability	Customer relationship digitization	Channel readiness
Supply chain and installed base security	Sourcing of unsecure components	Product, Project, System quality & Offer reliability	Inaccurate product information	Customer relationship digitization	Operations deployment
Supply chain and installed base security	Lack of source code governance	Brand management	Lack of (Social) media policy compliance	Customer relationship digitization	SC dematerialization

Third party screening and sanctions compliance	Non-compliance with Export control & Sanctions	Brand management	Lack of Branding policy compliance	Customer relationship digitization	Consultative selling
Third party screening and sanctions compliance	Lack of third party screening (incl. problematic local alliance and partners)	Brand management	Lack of Sponsorships and brand partnerships due diligence	SC flexibility and resilience	Inadapted evolution of the Supply Chain footprint
National security regulations	Lack of defense of Governmental industrial base (eg. FOCI mitigation)	P&L management	Unexpected losses	Organization	Unclear roles and Responsibilities
National security regulations	Lack of foreign Direct investment control (leading to an inability to invest)	P&L management	Unexpected variance vs forecast	Talent acquisition and retention	Competencies (e.g. lack of critical skills management)
Corporate governance	Corporate Officer's succession	Equity, diversity & Inclusion	Equity, diversity & Inclusion	Talent acquisition and retention	Talent attrition (e.g. war on talent)
Corporate governance	Board members' succession	Rewards & Benefits	Rewards & Benefits	Talent acquisition and retention	Lack of talent acqusition strategy
Corporate governance	Corporate Officer's misconduct and reputation	Development and competencies, Training, Wellbeing and Mental health	Lack of focus on Well-being and mental health	Performance mgmt	Lack of single source of truth for publication
Corporate governance	Board members' misconduct and reputation	Development and competencies, Training, Wellbeing and Mental health	Lack of competency planning (aligned with company strategy)	Performance mgmt	Auditability of non-financial performance (non-GAAP) metrics
Corporate governance	Corporate Officer's compensation	Development and competencies, Training, Wellbeing and Mental health	Lack of added value or relevant training resource	Performance mgmt	Lack of consistency of incentive plans vs group strategy and objectives
Corporate governance	Board members' compensation	Development and competencies, Training, Wellbeing and Mental health	Lack of deployment/enforcement of training	Offer creation process	Lack of innovation