

IRIS GLOBAL SERVICES LIMITED



IRIS GLOBAL

RISK MANAGEMENT POLICY

Under Regulation 17(9)(b) of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015

CIN: U72900DL2009PLC189527

Registered Address: 1, Bypass Road, Mahipalpur, 110037, New Delhi, India

For Iris Global Services Limited

Registration

Director

Page 1 of 10

INTRODUCTION

The Companies Act, 2013, emphasizes the requirement for a Risk Management Policy for the Company. Section 134(3)(n) of the Companies Act, 2013 requires that the report by the Board of Directors laid at the general meeting shall include a statement on the 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 shall be included in the Board's Report.

The Audit Committee is required to evaluate the internal financial controls and risk management systems of the Company, and the Independent Directors shall satisfy themselves that the systems of risk management are robust and defensible. Section 177(4)(vii) of the Companies Act, 2013 provides that the Audit Committee shall evaluate the internal financial controls and risk management systems of the company.

Regulation 17(9)(a) of SEBI (Listing Obligation and Disclosure Requirements) Regulations, 2015 ("**Listing Regulations**"), inter alia, mandates laying down the procedures for risk assessment and minimization. Further Regulation 17(9)(b) of the Listing Regulations, provides that the Board of Directors shall be responsible for framing, implementing and monitoring the risk management plan for the company.

Regulation 21(4) further provides that the board of directors shall define the role and responsibility of the Risk Management Committee and may delegate monitoring and reviewing of the risk management plan to the committee and such other functions as it may deem fit. Such functions shall specifically cover cyber security. It further states that the role and responsibilities of the Risk Management Committee shall mandatorily include the performance of functions specified in Part D of Schedule II. (**Annexure 1**)

The Board of Directors ("**the Board**") of [Iris Global Services Limited] ("**the Company**") has adopted the following policy, and the Board may amend this policy from time to time. In case of any subsequent amendments to the Regulations which make any of the provisions in the Policy inconsistent, the provisions of the Regulations shall prevail.

1. OBJECTIVE OF POLICY

The objective of this policy includes the following:

- Develop a risk culture that encourages all employees to identify risks, associated opportunities/gains and respond to them with effective actions;
- Develop both proactive and reactive mechanisms for risk management;
- Identify and manage existing/new risks in a planned and coordinated manner by the Risk Register and Risk Control Matrix;
- Develop an incident response management framework to manage the risks that may materialize;
- To enable compliance with appropriate regulations, wherever applicable, by adoption of best practices;
- To assure business growth with financial stability;
- Protecting and enhancing assets and Company image; and
- Reducing volatility in various areas of the business.

2. DEFINITIONS

"**Company**" means Iris Global Services Limited.

"**Risk**" means a probability or threat of damage, injury, liability, loss, or any other negative occurrence that may be caused by internal or external vulnerabilities; that may or may not be avoidable by pre-emptive action.

"**Risk Management**" is the process of systematically identifying, quantifying, and managing all risks and opportunities that can affect the achievement of a corporation's strategic and financial goals.

"**Senior Management**" means officers and personnel of the Company who are members of its core management team comprising all members of management one level below the Chief Executive Director or Managing Director or Whole Time Director, or Manager, including the functional heads, by whatever name called and the persons identified and designated as key managerial personnel, other than the board of directors, by the Company.

For Iris Global Services Limited

Signature

Page 2 of 10

Director

“Risk Management Committee” means the Committee formed by the Board as under Regulation 21 of the Listing Regulations.

Words and expressions used and not defined in this Policy shall have the meaning ascribed to them in the SEBI Listing Regulations, the Securities and Exchange Board of India Act, 1992, as amended, the Securities Contracts (Regulation) Act, 1956, as amended, the Depositories Act, 1996, as amended, or the Companies Act, 2013 and rules and regulations made thereunder.

3. RISK MANAGEMENT POLICY & FRAMEWORK

Risk is the potential for failure or loss of value or the missed opportunity for value creation / strategic competitive advantage resulting from either a certain action or a certain inaction.

Controlling risk is essential in any business by having processes to ensure the safeguarding of assets and compliance with appropriate regulatory frameworks. However, risks may also have to be taken consciously to explore untapped business opportunities in line with the corporate strategy to optimise maximum potential stakeholders' value and to improve their confidence.

Classification of Risks:

A. Financial / Operational / Preventable / Compliance risks:

These are internal risks, arising from within the organization that are controllable and need to be eliminated or avoided. The examples are:

- Governance, organisational structure, roles and accountabilities;
- Credit risk arising from customers and channel partners;
- Working capital and liquidity management;
- Inventory management and obsolescence risk;
- Vendor concentration and supply chain disruption risk;
- Human resource and talent retention risk;
- Information technology and infrastructure risks;
- Cybersecurity and data protection risks;
- Operational disruptions affecting sales, procurement, warehousing and distribution activities.

B. External risks

External risks come up due to economic events that arise from outside of an institution's control. It arises from the external events that cannot be controlled by any institution, cannot be forecasted with reliability, are normally beyond its control, and it is therefore difficult to reduce the associated risks. The examples are:

- Changes in laws, regulations and tax policies;
- Changes in technology trends and customer preferences;
- Macroeconomic conditions affecting IT spending;
- Intense competition in the technology distribution industry;
- Foreign exchange fluctuations impacting procurement costs;
- Supply chain disruptions caused by geopolitical events, pandemics, natural disasters or global semiconductor/component shortages;
- Changes in OEM partner strategies, product availability or distribution models.

C. Disruptive risks:

These are the anticipated or unanticipated events which may result in disruption of the operations of the firm or existence of its current business model, and innovations to business models that disrupt the existing paradigm- e.g. These are anticipated or unanticipated events that may significantly disrupt the Company's existing business model, operations or competitive position, including rapid technological advancements, emergence of new digital platforms, cloud-based procurement models, artificial intelligence-driven business transformations, cybersecurity incidents, changes in OEM distribution strategies, or disintermediation of traditional distribution channels.

For Iris Global Services Limited

Devi Vishwanath

Director

Strategic Risks:

Risks taken consciously are linked to strategic choices to earn a higher return. Strategic risks may arise from expansion into new technology segments, new geographic markets, cloud and managed services offerings, acquisitions, strategic partnerships, and investments in digital transformation initiatives.

The aggregate level and types of risk the Company is willing to assume within its risk capacity to achieve its strategic objectives and business plan shall be as per its risk appetite. The Risk Management process involves the following phases:

- Risk identification
- Risk evaluation and assessment
- Risk mitigation

3.1 Risk Identification

This involves continuous identification of events that may have a negative impact on the company's ability to achieve goals. The company has adopted a robust risk identification process, keeping in view the key activities/ focused areas of the company's business for the purpose of risk assessment. Identification of risks, risk events and their relationship is based on the basis of discussion with the senior management and analysis of related data/ reports, previous internal audit reports, past occurrences of such events, etc. The identification of risk by the company is broadly based on the following internal and external risk factors:

The risks can be broadly identified/ categorized into one or more following categories; however, the risk management committee may revise such categories:

Category of Risk	Examples
Financial Risks	- Financial misstatements/ improper accounting or financial reporting. - Unavailability of funding and cash flow; - Change in credit limit affecting availability of funds; - Market conditions on lending / borrowing of funds; - Loan repayment schedules not adhered; - Changes in the applicable laws and environment related to funding, investment norms, including raising of funds from international market;
Operational	- Business disruption; - Inefficient use of resources/increased product/ service cost; - Physical property/damage/disruption; - Accidents / force majeure events, change in management, etc. - Limited availability of manpower and resources;
Sectoral Risks	- Dependence on key OEMs, technology vendors and strategic partners; - Changes in vendor pricing, incentive programs and distribution - Customer concentration risk; - Competition from organised and unorganised distributors; - Supply chain and inventory management challenges; - Dependence on availability of technology products; and - Changes in enterprise IT spending patterns.
Sustainability (ESG Related) Risks	- Compliance with applicable environmental, social and governance requirements; - Employee welfare, diversity and workplace practices; - Responsible sourcing and ethical business practices;

For Iris Global Services Limited

Rajiv Kumar

Director

	Corporate governance and ethical conduct;
Information	- Leakage of confidential business, customer or vendor - Unauthorized access to sensitive commercial information; - Data privacy and data protection breaches; - Reputational damage arising from misinformation or adverse media coverage; - Intellectual property infringement risks.
Risks	- Disruption of IT operations; - Server issues; - Phishing, data leakage, hacking, insider threats, etc.
Cyber security risk	- Cyberattacks, ransomware and malware incidents; - Phishing and social engineering attacks; - Unauthorized access to networks, systems or databases; - Data breaches and privacy incidents; - Cloud security vulnerabilities; - Third-party technology service provider risks; - Disruption of IT infrastructure and business systems.
Strategic Risks	- Failure to adapt to evolving technologies and market dynamics; - Ineffective execution of growth strategies; - Loss of key vendor or customer relationships; - Damage to corporate reputation; - Failure of digital transformation initiatives
Compliance Risks	- Violation of laws or regulations governing areas including but not limited to: - Environmental; - Employee health & safety; - Labour laws; - Product quality/safety issues ; - Local tax and statutory laws. - Prosecution, fines, investigations, inquiries; litigation including class actions.

3.2 Risk Analysis

Risk analysis involves:

- consideration of the causes and sources of risk;
- the trigger events that would lead to the occurrence of the risks;
- the positive and negative consequences of the risk;
- the likelihood that those consequences can occur.

Factors that affect consequences and likelihood should be identified. Risk is analyzed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be taken into account.

For Iris Global Services Limited
Rajiv Kishan

3.3 Risk Assessment

Director

The Company evaluates risks considering their impact on revenue growth, profitability, cash flows, working capital requirements, vendor relationships, inventory position, customer retention, regulatory compliance,

information security, business continuity and reputation. 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 revenue, profit, balance sheet, reputation, business and system availability, etc., should the risk element materialize. The composite score of impact and likelihood is tabulated in an orderly fashion. 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 4 as follows.

Impact	Risk Level	Likelihood
Minor	1	Low
Moderate	2	Medium
High	3	High
Critical	4	Critical

3.4 Risk Mitigation

Risk treatment involves selecting one or more options for modifying risks and implementing those options. Once implemented, treatments provide or modify the controls.

Risk treatment involves a cyclical process of:

- Assessing a risk treatment;
- Deciding whether residual risk levels are tolerable;
- If not tolerable, generating a new risk treatment; and
- Assessing the effectiveness of that treatment.

Based on the Risk level, the company should formulate its Risk Management Strategy. The strategy will broadly entail choosing among the various options for risk mitigation for each identified risk. Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. The following framework shall be used for risk treatment:

1. Risk Avoidance (eliminate, withdraw from or not become involved)
Risk avoidance implies not starting or continuing with the activity that gives rise to the risk.
2. Risk Reduction (optimize - mitigate)
Risk reduction or "optimization" involves reducing the severity of the loss or the likelihood of the loss from occurring. Acknowledging that risks can be positive or negative, optimizing risks means finding a balance between negative risk and the benefit of the operation or activity, and between risk reduction and the effort applied.
3. Risk Sharing (transfer - outsource or insure)
Sharing, with another party, the burden of loss or the benefit of gain from a risk.
4. Risk Retention (accept and budget)
Involves accepting the loss or benefit of gain, from a risk when it occurs. Risk retention is a viable strategy for risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default. This includes risks that are so large or catastrophic that they either cannot be insured against, or the premiums would be infeasible. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great it would hinder the goals of the organization too much.

3.5 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

For his Global Services signed and

Rajiv Kishan

Director

of the internal auditors on a quarterly basis.

The statutory auditors carry 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 a regular periodic basis, the Board will, on the advice of the audit committee, receive the certification provided by the Managing Director and/or 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.

4. RISK MANAGEMENT COMMITTEE

The Risk Management Committee shall be responsible for framing, implementing and monitoring the risk management policy for the company. The Audit Committee should ensure that adequate risk management systems exist. The Risk Management Committee will be responsible for reviewing and action plan to mitigate these Internal, External and Strategic/Disruptive risks periodically and report to the Board of Directors accordingly.

The Risk Management Committee will discuss calculated risks required to be taken to augment strategic initiatives in a bid to achieve the long-term goals of the company. In a typical instance, the approach to setting and executing strategy might look at augmenting sales growth, exploring uncharted domestic/ international markets, tapping organic/ inorganic growth opportunities, elevating brand value or adopting evolving technological platforms for better service delivery.

Compliance with this Policy shall be the responsibility of the officer designated by the Board as Risk Officer or any other Key Managerial Personnel who has been the Chief Financial Officer of the Company, who shall have the power to ask for any information or clarification from the management in this regard.

The Audit Committee shall review risk management systems on an annual basis.

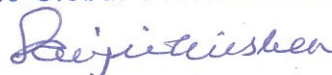
The Risk Management Committee shall comprise of:

- **Members:** Minimum three (3) members, with the majority of them being members of the Board of Directors, including at least one (1) independent director.
- **Chairperson:** Shall be a member of the Board and the senior executives of the Company.
- **Meeting:** The Committee shall meet at least twice in a year..
- **Quorum:** Shall be either 2 members or 1/3rd of the members of the Committee, whichever is higher, including at least 1 member of the Board to be present.

The terms of reference of the Risk Management Committee are as follows:

- a. to formulate a detailed risk management policy which shall include:
 - i. 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.
 - ii. Measures for risk mitigation including systems and processes for internal control of identified risks.
 - 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;

For Iris Global Services Limited



Director

- 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. review of strategic risks arising out of adverse business decisions and lack of responsiveness to changes;
- h. review of operational risks;
- i. review of financial and reporting risks;
- j. review of compliance risks;
- k. review or discuss the Company's risk philosophy and the quantum of risk, on a broad level that the Company, as an organization, is willing to accept in pursuit of stakeholder value;
- l. review the extent to which management has established effective enterprise risk management at the Company;
- m. inquiring about existing risk management processes and review the effectiveness of those processes in identifying, assessing and managing the Company's most significant enterprise-wide risk exposures;
- n. review the Company's portfolio of risk and consider it against its risk appetite by reviewing integration of strategy and operational initiatives with enterprise-wide risk exposures to ensure risk exposures are consistent with overall appetite for risk; and
- o. review periodically key risk indicators and management response thereto.

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.

5. ROLES AND RESPONSIBILITIES

The Risk Management Committee shall be responsible for framing, implementing and monitoring the risk management policy for the company. The Audit Committee shall review risk management systems on an annual basis and ensure that adequate risk management systems are in place.

6. REVIEW OF THIS POLICY

This Policy shall be reviewed by the Risk Management Committee periodically, at least once in two years, including by considering the changing industry dynamics and evolving complexity.

AMENDMENT

Any change in the policy shall be approved by the Board of the Company. The Board 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 in this respect shall be final and binding. Any subsequent amendment/modification in the Companies Act, 2013 or the rules framed thereunder or the Listing Regulations and/or any other laws in this regard shall automatically apply to this policy.

7. BUSINESS CONTINUITY PLAN

The Company's business continuity framework shall include disaster recovery procedures for critical information technology systems, cybersecurity incident response mechanisms, alternate supply chain arrangements, remote

Edisys Global Services Limited

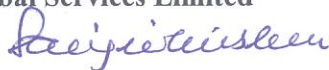
Rajiv Kishore
Director

working capabilities, data backup and recovery processes, communication protocols with customers, vendors and employees, and contingency plans for disruptions affecting procurement, warehousing, logistics and service delivery operations.

Business continuity plan refers to maintaining business functions or quickly resuming them in the event of a major disruption, in other words, a disaster management plan. The Company shall formulate a business continuity plan as may be required for protecting the interest of the Company in the event of happening/occurrence of any unforeseen events that may affect the business of the Company.

Such a business continuity plan may vary from time to time depending on the Company's needs and the risk management strategy being adopted by the company at such time. The business continuity plan may, among other things, focus on protecting the assets and personnel of the Company in the event of a disaster event which affects the day-to-day operations of the company's business. The business continuity plan may be reviewed and amended by the RMC from time to time, as the committee may deem fit.

For Iris Global Services Limited
For Iris Global Services Limited



Director

Version approved by: The Board of Directors

Date:

Place:

Note: Approved in the meeting dated 11th May, 2026

ANNEXURE 1

Role of Risk Management Committee

The role of the committee shall, inter alia, include the following:

1. To formulate a detailed risk management policy, which shall include:
 - 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.
 - Measures for risk mitigation, including systems and processes for internal control of identified risks.
 - 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 the 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;

The Risk Management Committee shall coordinate its activities with other committees in instances where there is any overlap with the activities of such committees, as per the framework laid down by the Board of Directors.

For Iris Global Services Limited



Director

