RISK MANAGEMENT POLICY

GLIDERS INDIA LIMITED

Corporate Office G.T. ROAD, Kanpur - 208013.

1. Back Ground

1.1 Gliders India Limited (GIL) will strive continuously to identify, evaluate, prioritize and minimize existing as well as potential risks related to business of the Company.

1.2 This Policy is in compliance with the requirements under Section 134(3) (n) of the Companies Act, 2013, which requires the Company to lay down procedure for risk assessment and procedure for risk minimization. The extract of the provision is reproduced below:

"Section 134 (3) (n) -A statement 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."

1.3 The Board of Directors of the Company will periodically review and evaluate the risk Management system of the Company so that the management controls the risk through properly defined network.

1.4 Head of Department /Unit head/GM/Sr.GM shall be responsible for implementation of the risk management system as may be applicable to their respective areas of functioning and report to the Board.

2. Purpose

2.1 The purpose of the Risk Management Policy is to enable and support the Board in structured and effective management of Risks.

3. Approach

3.1 Considering the status of various programs, projects and the emerging business scenario where a level playing market field is being created in the defense industry, a philosophy that must consistently guide the company's risk management approach is given below:

"Empowering business growth and competitiveness through strategic and structured Risk taking and sustained risk mitigation"

3.2 This philosophy implies Risk Management will be applied in a transparent environment, to sustain the business growth and profitability in a competitive market through structured risk taking and risk mitigation processes.

3.3 These processes will strengthen Technology Absorption and Development, product delivery, service and up-gradation, substantive self-reliance, Product Availability and affordability. This philosophy will be driven by a risk aware mindset where avoidance of necessary risks is discouraged.

3.4 The Risk Management Policy will initially keep the processes flexible to enable the users to adapt to their needs. All GM/ HOD's will also present a feed forward map of the potential risks in the Political, economic, government policy, social and market/technology environment for the Board to consider changes in strategies and plans that may be required.

3.5 Risks shall be addressed effectively at each level through an appropriate organization and commensurate allocation of resources.

4. Scope

4.1 Significant proposals that are approved by GM/ HOD's/ MDs / Board will contain a summary of the Risk Assessment in the proposals and the Risk mitigation plans that are built into the proposals. Here significance implies short term and long term impact on financial and strategic parameters.

4.2 GIL is continuously exposed to risk due to globalization of business environment, fast changing technology and changes in Government Policies.

4.3 Risk Management Policy ("RMP") objectives is to facilitate a common understanding of risk at early stage for effective mitigation to meet company's business goals.

4.4 The Mitigation measures identified shall be embedded suitably into business process of the Company.

4.5 An effective Risk Management process is the key to sustained operations there by protecting the shareholder value, improving governance process, achieving strategic

objective and being well prepared for adverse situation or any unforeseen circumstances, if it occurs in business activities of the Company.

4.6 The main objective of this Policy is to ensure sustainable business growth with stability and to promote a pro-active approach in reporting, evaluating and resolving risk associated with the business.

5. Areas of Risk Management

5.1 **Risk:** Risk is an event that is likely to occur, which can potentially have an adverse impact (consequence) on the planned outcomes of a proposal, project or business decision. A Risk can be a result of unintended outcomes of well-reasoned decisions also.

5.2 Risks are normally assessed subjectively and initially dialogue would be required to arrive at the Risk level.

5.3 GIL has identified the following indicative major area of risk related to:

- ✓ Finance
- ✓ Operations
- ✓ Product Portfolio
- ✓ Market
- ✓ Human resource
- ✓ Technology
- ✓ Cyber Security
- ✓ Enterprise as a whole

6. Methodology for Risk Management

6.1 The risk associated to business emerge due to various internal and external factors need to be identified, evaluated, prioritized and managed. Mitigation Measure need to be finalized and need to be incorporate in business process and practices followed by the Company.

6.2 Further, **risk mitigation measures already incorporated in business process will be reviewed on half yearly basis by the Board Level and quarterly basis by the respective Unit heads**, to check their effectiveness.

6.3 Every year the area of risk shall be identified, prioritized and focused efforts shall be made to assess & mitigate the risks.

7. Risk Management Process

7.1 Risk Management ("RM") process is identified as important business management process. It is a continuous and developing process, which encompasses the organization's strategy and implementation of Strategy. It will cover all important risk associated with business of the GIL, which arise out of internal and external factors.

7.2 **Risk Management approaches to manage a potential risk are:**

a. **Avoid:** Avoid risk that involve a high probability impact for both financial loss and damage.
b. **Transfer:** Risk that may have low probability for taking place but would have a large financial impact to be mitigated by being shared or transferred, e.g. by purchase of Insurance or outsourcing etc.
c. **Accept:** Risk, where the expense involved in mitigating the risk is more than the cost of tolerating the risk should be accepted.
d. **Limit:** Risk limitation, to be considered to address a perceived risk and regulate their exposure. The risk limitation involves some risk acceptance and some risk avoidance.

7.3 The following steps to be followed for RM process:

a. Risk Assessment: it covers identification of risk, risk estimation & evaluation.

Risk Identification:

The first step in risk assessment is risk identification based on organizational process and key driver of the risks. The indicative key drivers can be categorized as below in table:

Indicative key drivers

Type of Risks	Due to Internal Drivers	Due to External Drivers	Due to both Internal & External Drivers
Financial Risk	-Liquidity -Treatment of Taxation -Insurance -Financial Management & Planning	-Inflation -interest rate -Credit worthiness of partner/stakeholders -Geo Political Developments	Return on Investment
Operations Risk	-Information/ERP System -Plant & Machinery -Material & Components	-Regulations -Vendors/partners -Environmental Risk	-Supply Chain -Power & Water supply -Strike and Lockout

	-Order Book Position		
Product Portfolio Risk	-Time of Market -Quality -Reliability -Product diversification -Product Marketing	-Product liability -Compliances and regulations -Demand Risk -Price Risk -Potential Customer acquisition	-Customer Experience -Reputation
Market Risk	-Understanding the market -Market diversification -Pricing of Market -Customer Acquisition strategy	-Type of Market system - Competition/ Competitors -Customer preference -Technology	-Customer Expectation -Brand Risk
Human Resource	-Organization culture -Employee relation -Talent retention -	-Societal culture -Demand for talent -legal Compliances	-people's aspiration -recruitment
Technology Risk	-Selection of technology -Development/ Acquisition of technology	-Disruptive Technologies -Technology Obsolescence	-Regulatory framework/ compliances -IP right/protection -Technology Gap
Cyber Security Risk	-Failure of IT system -Security breach -Unauthorized access -Privilege creep	-Cyber attack -Distributed Denial of Services (DDoS) -Malware/ Computer virus, phishing attack etc	-Cyber security technology lagging behind cyber fraud -Breach in cyber security in the supply chain -Cyber security risk due to convergence in business process
Enterprise Risk	-R&D Investment -Intellectual Property -Assets Utilization -Controls/Procedures -System & process	-Competition -Industry changes -Market Economic -Govt. policies	-M&A integration -Partnerships -Litigation/ Arbitration -Company public relation

b. Risk Estimation & Evaluation

This can be quantitative, semi-quantitative or qualitative in terms of occurrence and possible consequences. The *"Risk Estimation"* to be carried out as per format issued with approval of Functional Director/Unit Level.

c. Risk Reporting & Treatment

Unit of GIL shall ensure that reporting of Risk Management assessment and their mitigation/treatment plan shall report to Board Level on quarterly basis.

d. Monitoring & Review

- This Policy shall evolve through review of the Audit Committee and the Board from time to time as may be necessary.
- This Policy will be communicated to all vertical/functional heads and other concerned persons of the Company.

8. RISK APPETITE FRAMEWORK

8.1. Risk appetite can be defined as the amount and type of risk that an organisation is willing to take in order to meet its objective. Risk appetite is the total risk that the organisation can bear in a given profile, usually expressed in aggregate term. It refers to a longer term strategy of the organisation.

8.2. Efforts shall be made to minimize risk exposure, while accepting and encouraging an increased degree of risk in pursuit of its vision and strategic goal and objective. It recognise that appetite for risk varies according to the activity undertaken and that acceptance of risk will be taking into consideration the potential benefit and deployment of measures to mitigate risk.

8.3. The functional director may fix the appetite level for factory unit, training academy and corporate level and risk appetite may be reviewed after every one-year interval.

9. Suggested Approaches to Mitigation Plan for risk

A few of the High impact risks that can affect the company's revenues and market share in the future and their mitigation plans are given below:

9.1 Mitigation for Risks in Product Performance

9.1.1 Contract related Risks and weaknesses should be addressed through a team of CO consisting of Planning, Contracts Cell and Legal cell. They may address review gaps in contracting leading to weaknesses in selecting the technology or inadequate depth in transfer of technology or in delays in receiving technology for product support. These gaps may be plugged to the extent feasible, in all new contracts yet to be signed.

9.1.2 Risks in technology processes and competencies including risks of quality failures due to improper / inadequate inspection or inadequate supervisions should be addressed by Senior GM / GMs / COPs through Mitigation plans and reported to the appropriate higher authorities or management. Where feasible the use of IT to strengthen these practices may be followed. Due diligence needs to be ensured to distinguish between systemic and personal causes of the risks to avoid individual blame.

9.2 Mitigation for Risks in Product Delivery

9.2.1 Any potential Risks of inadequacy of Project team formation (including planned strength and competencies) should be addressed by the respective Senior GM / GM or MD / CEO and reported to the appropriate higher authorities or management. Similarly, any other risks that may arise, which can have an impact on product or service delivery including liquidated damages, inventory holding should be addressed by the respective Senior GM / GM / CEO of the Unit (OPF) in consultation with Financial consultant and reported to the appropriate higher authorities or management. Risks due to development of critical must be assessed, including Vendor delivery related risks. Mitigation plans for ensuring that product delivery is not affected by the delays in the development and certification of the systems and sub- systems. They must be reviewed and redrawn to ensure effectiveness of the mitigation plans.

9.2.2 A policy on indigenization is required to be established to prevent destabilization of supplies due to recertification delays.

9.2.3 It is recommended that Risks relating to Purchase and outsourcing across multiple Divisions should be reviewed by the respective COPs or program managers every year and reported to the appropriate higher authorities or management.

9.2.4 Risks on account of Force Majeure clauses should also be indicated wherever applicable, by the respective Purchasing or Outsourcing department heads, in terms of

their impact on product delivery and realization of payments. Their recommendations for plans for such risk mitigation should be reviewed.

9.3 Mitigation for Financial Risks

9.3.1 The respective finance heads should create an appropriate mechanism and financial information system for capturing the risks of cost overrun and bringing it to the attention of the Divisional / Project / Program management. Finance & IMM Head of the Division may also discuss in Divisional Committee of Management meeting on the aspects of budget monitoring, System Audit Reports, etc.

9.3.2 The Corporate Finance group will submit an assessment of the risks due to excessive Reserves and Surpluses, Cash and Bank Balances which are not in line with the business needs in gainfully deploying surpluses (to prevent a risk aversive mindset).

9.3.3 A Corporate annual SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis will be presented to the MC by Corporate Planning group for review of the strategies and for initiating and strengthening focused mitigation actions on risks arising out of Threats including threats arising out of current and potential competition for expected orders.

9.3.4 Financial risks arising out of Design and Development efforts with or without orders must be assessed and mitigation plans be prepared by the Corporate Planning group.

9.4 Mitigation of HR Risks

9.4.1 Risks on talent acquisition, retention, engagement and Knowledge Management should be addressed by CO HR and reported to HR Sub- committee of the Board.

9.5 Mitigation of Corruption Risks

9.5.1 The Corporate Vigilance Office will consolidate the corruption risks identified by Corporate Vigilance and submit and suggest measures to mitigate minimize / eliminate and control corruption risks.

9.5.2 The Corporate Vigilance Department will forward Annual Report on status of complaints received and cases of violations of CRM Policy to Risk Cell for submission to the Management Committee & Audit Committee.

9.6 Mitigation of Legal Risks

9.6.1 CO Legal Section and Company Secretariat will review the risks arising out of practical difficulties involved in legal and statutory compliances and the mitigation plans required will be prepared by the respective Divisional / Complex offices.

9.7 Mitigation of Cyber Security Risks

9.7.1 As part of the IT Security Policy of the company, Cyber Security Risks will be presented to RMC along with existing risk reporting template of RMP.

9.8 Mitigation of Business Continuity Plan (BCP) Risks

9.8.1 A template for checklist for BCP of the company will be prepared and reviewed at regular intervals which covers up different parameters. The Divisions as part of ISO 9001:2015(E) will include BCP. Compliance will be submitted in the annual review by RMC.

9.9 Annual Review

9.9.1 Risks will be placed for review by the Risk Management Committee periodically covering inter-alia the following:

a) Operational Risk by DRMC (Disaster Risk Management Cycle)
b) Strategic Risk by Corporate Planning
c) Cyber Security Risk by CO-IT (Cyber security cell)
d) Compliance of BCP (Business Continuity Plan)

10. Audit committee

10.1. Audit Committee, if any, shall be evaluated the Risk Management System. The Board may define the roles and responsibilities of the Audit Committee in addition to prescribed under the Companies Act, 2013 & DPE Guidelines. It may also delegate monitoring and reviewing of the risk management plan to the committee and such other functions as it may deem fit.

11. Role of Board

11.1. The Board shall be responsible for formulation, implementing and monitoring the risk management plan for the Company.

11.2. The Board shall define the roles and responsibilities of the Audit Committee and may delegate monitoring and reviewing of the risk management plan to the Committee and such other functions as it may deem fit.

11.3. Ensure that the appropriate systems for Risk Management are in place.

11.4. The Independent Directors shall help in bringing an independent judgment to bear on the Board's deliberations on issues of risk management and satisfy themselves that the systems of risk management are robust and defensible.

11.5. Participate in major decisions affecting the organization's risk profile.

11.6. An awareness of and continually monitor the management of strategic risks.

11.7. An appropriate accountability framework is working whereby any delegation of risk is documented and performance can be monitored accordingly.

11.8. Ensure Risk Management is integrated into Board reporting and Annual reporting mechanisms.

11.9. Convene any Board-committees that are deemed necessary to ensure risk is adequately managed and resolved where possible.

12. Disclosure in Board 's Report

12.1 Board of Directors shall include a statement indicating development 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.