NIVA BUPA HEALTH INSURANCE COMPANY LIMITED

RISK MANAGEMENT POLICY

NIVA BUPA HEALTH INSURANCE COMPANY LIMITED

RISK MANAGEMENT POLICY

1. PREAMBLE

1.1 Niva Bupa Health Insurance Company Limited ("the Company" or "Niva Bupa") has formulated this Risk Management Policy ("Policy") to ensure effective navigation to achieve business objectives and enable sustainable growth in a volatile and complex environment. The Company's risk management framework has been designed to identify, monitor and minimise the adverse impact of *inter alia* strategic, operational, technological, financial, regulatory and compliance risks faced by it.

1.2 Risk is defined as the threat or probability of an action or event which adversely affects Niva Bupa's ability to achieve its objectives and/or to complete day to day activities in a manner which is consistent with legal, regulatory, customer and shareholder expectations.

1.3 The Company's risk management framework ensures a consistent, collaborative, and comprehensive approach and framework to identify, assess, measure, prioritise, respond and monitor various kinds of risks and report the same to the Audit Committee and the Board for review and discussion and enable them to take informed decisions and suggest actions and strategies to mitigate those risks.

1.4 This Policy is guided by the principles and objectives as enumerated in Regulation 21 read with Part D of Schedule II of SEBI LODR Regulations, Section 177 of the Companies Act, and based on the Corporate Governance Guidelines for Insurance Companies issued by Insurance Regulatory Development and Authority of India dated 18 May 2016 (herein referred as "**IRDAI Guidelines**") and all other applicable provisions made thereunder, as amended from time to time.

2. PURPOSE

2.1 This Policy aims to ensure that the Company adopts a robust, consistent and calibrated approach towards the identification, assessment, measurement, analysis and control of the key risks that could threaten the assets, solvency, earning capacity, business objectives or reputation of the Company.

2.2 This Policy reflects the primary objective of risk management framework to ensure a sustainable business growth with stability by establishing a structured and comprehensive approach to risk management at the Company.

3 DEFINITIONS

3.1 **"Board"** means Board of Directors of the Company;

3.2 "**Companies Act"** means the Companies Act, 2013 and rules made thereunder, as amended from time to time;

3.3 **"Company"** or "**Niva Bupa**" means Niva Bupa Health Insurance Company Limited (formerly known as Max Bupa Health Insurance Company Limited;

3.4 **"Director"** means a director appointed to the Board of the Company;

3.5 **"Independent Director"** means a director referred to in Section 149 (6) of the Companies Act;

3.6 "**IRDAI**" shall mean Insurance Regulatory and Development Authority of India;

3.7 "**IRDAI Guidelines**" means guidelines issued by IRDAI on Corporate Governance for insurance companies dated 8 May 2016, as amended from time to time;

3.8 **"Key Management Person"** as defined under IRDAI (Registration of Indian Insurance Companies) Regulations, 2022 read with Corporate Governance Guidelines for Insurance Companies issued by IRDAI means members of the core management team including all Whole-time Directors, Managing Directors, Chief Executive Officer, and the functional heads one level below Chief Executive Officer/ Managing Director, including the Chief Financial Officer, Chief Investment Officer, Chief Risk Officer, Chief Compliance Officer and the Company Secretary;

3.9 "**Policy**" means this Policy for risk management of the Company;

3.10 "**Risk Management Committee**" or "**Committee**" means the committee set up in accordance with para 4 of this Policy; and

3.11 **"SEBI LODR Regulations"** means the Securities Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations 2015, as amended from time to time.

4 CONSTITUTION OF THE RISK MANAGEMENT COMMITTEE

4.1 The Committee shall consist of a minimum of 3 (three) members with majority of them being members of the Board, including at least 1 (one) Independent Director. The Chairperson of the Risk Management Committee shall be a member of the Board and senior executives of the Company, may be the members of the Risk Management Committee.

5 ROLE OF THE RISK MANAGEMENT COMMITTEE

5.1 The role of the Risk Management Committee shall be:

a) To formulate a detailed framework for identification, assessment, measurement and analysis of internal and external risks specifically faced by the Company in particular including strategic, financial, operational, technological, regulatory and compliance, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the Committee;

b) To provide measures for risk mitigation including systems and processes for internal control of identified risks;

c) To formulate business continuity plan;

d) To ensure that appropriate methodology, processes and systems are in place

to monitor and evaluate risks associated with the business of the Company;

e) To monitor and oversee implementation of this Policy, including evaluating the adequacy of risk management systems;

f) To periodically review this Policy, at least once in 2 (two) years, including by considering the changing industry dynamics and evolving complexity;

g) To keep the Board informed about the nature and content of its discussions, recommendations and actions to be taken;

h) To provide framework for the appointment, removal and terms of remuneration of the Chief Risk Officer;

i) To review the Company's risk governance structure, risk assessment and risk management policies, practices and guidelines and procedures, including the risk management plan;

j) To set the risk tolerance limits and assess the cost and benefits associated with risk exposure;

k) To review the Company's risk-reward performance to align with overall policy objectives;

l) To discuss and consider best practices in risk management in the market and advise the respective functions;

m) To assist the Board in effective operation of the risk management system by performing specialized analyses and quality reviews;

n) To maintain an aggregated view on the risk profile of the Company for all categories of risk including insurance risk, market risk, credit risk, liquidity risk, operational risk, compliance risk, legal risk, reputation risk, etc;

o) To advise the Board with regard to risk management decisions in relation to strategic and operational matters such as corporate strategy, mergers and acquisitions and related matters;

p) To report to the Board, details on the risk exposures and the actions taken to manage the exposures;

q) To review, monitor and challenge where necessary, risks undertaken by the Company;

r) To review the solvency position of the Company on a regular basis;

s) To monitor and review regular updates on business continuity;

t) To review disclosure statement in any public documents or disclosures;

u) To formulate a fraud monitoring policy and framework for approval by the Board;

v) To monitor implementation of Anti-fraud policy for effective deterrence, prevention, detection and mitigation of frauds;

w) To review compliance with the guidelines on Insurance Fraud Monitoring Framework dated 21 January 2013, as amended or reissued by IRDAI from time to time;

x) 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.

6 POLICY REQUIREMENTS

6.1 Application

a) To comply with this Policy, all Niva Bupa's offices and functions, in line with Niva Bupa's Risk Management Framework,

shall meet at least every quarter, to formally review the key risks that have, or may give rise to, significant loss events and document them and undertake the following actions:

- Analyse these key risks in terms of probability and impact;
- Assess these key risks against a pre-defined risk appetite to establish any necessary control action(s);
- Assess the residual risk position;
- Develop and implement an appropriate and cost -effective risk management plan to bring these risks within appetite;
- Track and report to the Committee on the progress of risk mitigation actions within the risk management plan;
- Retention of risk must be aligned with the risk mitigation strategy whereby it is commercially and economically appropriate to do so;
- Identify, assess market related risks, and vulnerability in digital infrastructure and cyber threats;
- Assess corporate accounting fraud, financial reporting, compliance with applicable laws, rules and regulations;
- Assess project quality, implementation and delay in commissioning.

b) The quorum for a meeting of the Risk Management Committee shall be either 2 (two) members or 1/3rd (one third) of the members of the Committee, whichever is higher, including at least 1 (one) member of the Board in attendance.

7 RISK MANAGEMENT FRAMEWORK

PROCESS

7.1 Risk management is a continuous process that is accomplished throughout the life cycle of a Company. It is an organized methodology for continuously identifying and measuring the unknowns; developing mitigation options; selecting, planning, and implementing appropriate risk mitigations; and tracking the implementation to ensure successful risk reduction.

7.2 A framework for identification of internal and external risks 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 Committee shall be prepared.

7.3 All Niva Bupa's offices and functions shall refer to the Risk Management Framework which comprises of following elements:

a) Strategic Risk Assessment;

b) Risk Strategy and Risk Appetite Statements;

c) Risk Categories;

d) Risk Registers;

e) Risk and Control Self-Assessment;

f) Risk Reporting; and

g) Risk Management design and effectiveness review

7.4 **Strategic Risk assessment** is the process of risk prioritization. The potential impact may include 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.

- External risks factors:
  - Economic Environment
  - Political Environment
  - Changes in laws and regulations
  - Competition
  - Fluctuations in input material
  - Changes in technology
  - Changes in government policies
  - 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.

- Internal control is exercised through policies and systems to ensure timely

availability of information that facilitate pro-active risk management.

- Internal risks factors
  - Project Execution
  - Contractual Compliance
  - Operational Efficiency
  - Hurdles in optimum use of resources
  - Quality Assurance
  - Environmental Management
  - Human Resource Management
  - Culture and values

- Financial risk – The financial risks relate to adequate liquidity for routine operations and availability of funds for expansions, impact of currency fluctuations, change in credit ratings, etc. It also includes the risks associated with the investments of the Company. The investments of the Company should be made on the basis of financial modelling and the currency fluctuations be examined regularly.

- Sectoral risk - The sectoral risk refers to the influence of industry variables such as demand-supply outlook, input risk, input cost fluctuation, competition, utilisation levels along with the impact of government regulations and policies on the Company.

- Compliance Risks: Risk of loss resulting from legal and regulatory factors such as Legal Risks & Health, Safety and Environmental Risks.

- IT-related Risks: Risk of technological challenges and other cyber security risks such as technological risks including hardware and software failure, human error, spam, viruses and malicious attacks and cyber security risks such as ransomware, phishing, data leakage, hacking, insider threats.

7.5 **Risk Categories** is to be conducted taking the existing controls into consideration. Risk events assessed as "high" or "very high" criticality may go into risk mitigation planning and implementation; low and medium critical risk to be tracked and monitored on a watch list.

7.6 **Risk and Control Self-Assessment**- To ensure that the above risks are mitigated, the Company will strive to:

- Involve all functions in the overall risk identification and mitigation exercise;

- Link the risk management process to the strategic planning and internal audit process;

- The Risk Management Committee shall have access to all information necessary to fulfil its responsibilities. It has the powers to seek information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise, if it considers necessary;

- The Risk Management Committee may in its judgment periodically commission risk management analysis of the Company;

- Adequate disclosures pertaining to the risks being faced by the Company, may be made as per the materiality criteria defined in the 'Policy for determination of materiality for disclosure of events or information' of the Company.

7.7 **Risk Reporting**- Functional heads are required to report the results of their periodic risk assessments, along with relevant supporting commentary, in line with the timetable laid down under the Risk Management Framework. The results of the risk assessments will be reported to the Risk Committee on a quarterly basis. Every head of Departments or such other authorized persons by Board shall also give details regarding any apparent risk and prospective opportunities relating to their departments on periodic basis to the Board.

7.8 **Risk Management design** uses the output of a risk assessment and implements countermeasures to reduce the risks identified to an acceptable level. This Policy provides process of assessing and mitigating risks identified within functions and associated processes. In circumstances where the accepted risk of a particular course of action cannot be adequately mitigated their status shall be continuously monitored and periodically presented to Risk Management Committee and Audit Committee.

8 GOVERNANCE

8.1 The risk management function shall be under the overall guidance and supervision of the Chief Risk Officer ("**CRO**"). The CRO shall be working closely with the Board, Audit Committee and shall be responsible for developing and implementing risk assessment policies, monitoring strategies, and implementing risk management capabilities.

8.2 The CRO's shall help the Board and executive management to determine the risk-reward trade-offs in the business and bring unfettered transparency into the risk profile of the business.

8.3 The CRO will be supported by a team of risk analysts and shall work closely with the business units, functional heads to identify risks and then evaluate and negotiate risk response plans based on cost-benefit analysis.

8.4 The CRO shall monitor all the risks across the various lines of business of the Company including compliance under applicable laws, finance functions, and other operating functions of the Company.

8.5 Individual and organisational responsibilities are outlined at **Annexure I.**

8.6 The risk management team will provide support to ensure consistent and effective implementation of this Policy and provide objective assurance as to Niva Bupa-wide compliance with this Policy.

8.7 The CRO shall ensure that all outsourcing arrangements of the Company shall have the approval of a Committee of Key Management Persons and shall meet the terms of the Board approved outsourcing policy.

8.8 The Board or the Risk Management Committee shall periodically be apprised about

the outsourcing arrangements entered into by the Company and also confirm to the effect that they comply with the stipulations of IRDAI as well as the internal policy be placed before them.

8.9 The CRO shall ensure that every outsourcing contract shall contain explicit safeguards regarding data protection including collection, storage, processing, retrieval, deletion and confidentiality of data and all outputs from the data, continuing ownership of the data with the Company and orderly handing over of the data and all related software programs on termination of the outsourcing arrangement.

8.10 The CRO shall ensure that the management of the Company monitors and reviews the performance of agencies to whom operations have been outsourced at least annually and report findings to the Board.

9 REPORTING ARRANGEMENTS

9.1 The Board shall include 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 in its Board Report.

9.2 The Board of the Company and the Audit and Risk Management Committee shall periodically review and evaluate the risk management system of the Company, so that the Management controls the risks through risk management framework.

10 DISCLOSURE ON THE WEBSITE OF THE COMPANY

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

11 INTERPRETATION

11.1 In all circumstances where the terms of this Policy are inconsistent with any existing or newly enacted law, rule, regulation, or standard governing the Company, the said law, rule, regulation, or standard will take precedence over this Policy.

11.2 Any and all terms which been defined under the Companies Act and/or the SEBI LODR Regulations (including subordinate legislations thereunder) shall be construed as per such definitions in these laws.

Annexure I: Key Responsibilities

Risk Committee of the Board	• Reviews and approves the Risk Management Policy • Reviews and approves the Risk Management Framework • Reviews and approves the Company's risk appetite statement • Monitors the Company's risk profile and recommend actions as they see appropriate
1st Line of Defence (Function Owners/ Functional Heads)	• Set the strategy of the Company • Deliver the business plan considering all applicable risks • Operate within the defined risk strategy and appetite • Conduct risk identification and assessment as per the defined framework • Design and implement controls • Conduct self- assessment of the available controls • Identify the mitigation plans and execute them to mitigate risks • Report the gaps/ deviations and correct them
2nd Line of Defence Chief Risk Officer	• Define the Risk Management Framework • Advice, support and challenge the 1st line of defence in the risk identification and assessment process • Advice the Management on setting the risk strategy and appetite • Conduct independent assessment of the controls deployed and advice on effectiveness • Monitor the identified mitigation plan • Specify the risk reporting and escalation thresholds • Report the Company risk profile to the Board and other relevant committees also covering any risks that fall outside the approved risk appetite of Niva Bupa
3rd Line of Defence (Internal Audit)	• Assessment of the effectiveness of Risk Management frameworks and processes