RISK MANAGEMENT POLICY

Rev 1.2

FSN E COMMERCE VENTURES LIMITED

May 2024

NYKAA

Table of contents

I. Setting the context

In a rapidly changing business environment with dynamic and shifting customer preferences, complexities in the regulatory landscape, and cyclicality in the macro-economic environment, business risks are also constantly evolving.

Risks are uncertainties that affect the achievement of strategic business objectives.

At Nykaa, while we scan the business horizon to evaluate potential business opportunities, we also continuously monitor the internal and external environment to identify, assess and mitigate potential risks. These include those arising from Geo-political and macro-economic factors, shifting Consumer preferences, Employee health & safety, Environmental & Social considerations, Competition, Legal & Regulatory, People, Technology, Information Security & Cyber risks that may adversely harm or threaten the achievement of our strategic objectives.

To effectively mitigate risks that impact our strategic business objectives, we have employed an enterprise-wide risk management framework by adapting the frameworks of COSO Enterprise Risk Management (ERM) framework 2017 as also ISO 31000 Risk Management framework, to support in the proactive identification, assessment, prioritisation, management and monitoring of risks that could have a material impact on the achievement of Nykaa's business objectives, while also formulating relevant risk mitigation strategies which helps protect our assets, and support informed decision making to reduce the impact of any adverse events.

Our Risk Management policy is based on our organisational vision and strategic goals and is specifically designed, to achieve the following objectives:

i. Ensure achievement of the Company's vision and strategic priorities in line with its core values.
ii. Integrate risk management in the culture and strategic decision-making in the organization with a view to build organisational resilience.
iii. Enable compliance with appropriate regulations and adoption of leading risk management practices.
iv. Anticipate and respond to changing political, economic, social, technological, legal, and environmental conditions in the external environment.

ERM aims at ensuring that key decisions regarding strategy and institution building are commensurate with the Company's risk appetite.

II. Applicable regulatory requirements in India

Section 134(3)(n) of the Companies Act, 2013 ("Act") requires a statement to be included in the report of the board of directors ("Board") of FSN E-commerce Ventures Limited ("Nykaa" or the "Company"), indicating 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.

Furthermore, **Regulation 17(9)(b) of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015** ("Listing Regulations"), as amended, 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. The responsibilities of the Board of Directors of the listed entity include inter-alia reviewing and guiding the risk policy of the entity.

This policy sets out the Board's requirements in relation to the establishment of and compliance with a framework for facilitating the management of business risks effectively, consistently and in line with the Company's risk appetite.

III. Nykaa's Enterprise Risk Management (ERM) framework

The Enterprise Risk Management framework at Nykaa is inclusive, well integrated, and standardized, and embraces the underlying principles of the COSO ERM framework & ISO 31000 Risk management processes to encompass all relevant facets of the business.

The framework enables the Company to strike an optimal balance between its growth and associated risks in pursuit of its strategic and operational business objectives.

Nykaa's risk management process strives to identify and analyse all significant risks that could potentially disrupt the business operations across the value chain keeping in mind short term as well as long term risks, as well as emerging risk areas.

Risks are identified and measured based on their nature, likelihood of occurrence and its associated potential impact. Mitigation action plans are built to manage material risks, and the effectiveness of risk management strategies are continuously monitored.

Our risk management approach is composed primarily of three components:

i. Risk Governance
ii. Risk identification and mitigation
iii. Risk management processes

i. Risk Governance:

a. Risk Management Committee:

The Risk Management Committee of the Board is constituted with the overall responsibility of overseeing and reviewing risk management processes across the Company. The risk management committee shall meet at least twice in a year, and the meetings of the risk management committee shall be conducted in such a manner as may be prescribed in the Listing regulations from time to time.

Terms of reference of the Risk Management Committee:

a. To review the risk management policy periodically - at least once in two years, also factoring the changing industry dynamics and evolving complexities in the business landscape. The policy shall include *inter-alia*:

   i. A framework for identification of internal and external risks specifically faced by the Company that could adversely impact the attainment of strategic objectives including geopolitical, sectoral, political, social, financial, operational, sustainability (particularly environment, social and governance related risks), regulatory, information security & cybersecurity risks *or* such other risk factors as may be determined.

   ii. Measures for risk mitigation including systems and processes for internal controls to mitigate identified risks.

   iii. Business Continuity.

b. To review whether appropriate methodologies, processes and systems are in place to identify, evaluate, treat and / or monitor risks associated with the business and approve such framework.

c. To review and approve risk tolerance and appetite levels, recognizing contingent risks, inherent and residual risks, and to assess whether current exposure to the risks the Company faces is acceptable and whether the Company has an effective risk mitigation process on an on-going basis.

d. To oversee and monitor the implementation of the risk management policy, and the Company's compliance with the risk management framework, including evaluating the adequacy of risk management systems and processes.

e. To approve major decisions affecting the risk profile or exposure of the Company and give appropriate guidance for risk mitigation with a view to balance risks and opportunities, as also evaluate the effectiveness of decision-making process in crisis and emergency situations.

f. To generally assist the Board in the execution of its responsibility for oversight and governance of risk and keep the Board of Directors informed about the nature and content of its discussions, recommendations, and actions emanating from Risk Management committee meetings.

g. The Risk Management Committee shall coordinate its activities with other Board committees, in instances where there is any overlap with activities of such committees, as also attend to such other matters and functions as may be prescribed by the Board from time to time.

h. To consider the terms of appointment or removal of as also remuneration of the Chief Risk Officer (if any, appointed)

i. To have powers to seek information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise, if and where it considers necessary.

   and

j. To comply with such other terms of reference as may be prescribed under the Companies Act 2013 and / or SEBI (Listing Obligations and Disclosure Requirements) Regulations, periodically.

b. *Risk Steering committee:*

The Risk Steering Committee is an internal management group responsible to ensure effectiveness of the overall Enterprise risk management process. This forum will be headed by the Executive Chairperson & Managing Director and Chief Executive Officer ("MD & CEO") of the Company, or such senior leader who may be nominated by the MD & CEO to steer the committee.

The composition of the steering committee will include the Business Heads of the respective business verticals, as also members of the Senior Leadership team who may be invited to participate in the risk steering committee meetings on a need basis.

The CFO, CHRO, Head of Legal, and the CTO will be permanent invitees to the committee.

Terms of reference of the Risk Steering Committee:

a) To review the design of and support in the implementation of the risk management processes within the organisation.
b) To review the risk profile of the Company periodically and recommend necessary actions to manage the downsides, as may be identified from time to time.
c) To implement the Risk management policy within the Company and develop a risk intelligent culture that enables the organisation to build resilience to critical business risks.
d) To provide support in identifying relevant high priority risks, define appropriate risk mitigation strategies and review status of its mitigation action plans including Business Continuity on a periodic basis.

To facilitate the above, the Risk Steering Committee will be assisted by the Head of the Internal Audit and Risk Management function.

The internal risk steering committee will have its meetings once in every quarter.

The outcomes of the discussions will be presented at the Risk Management committee of the Board.

c. *Risk management function:*

The Head of Internal Audit and Risk Management function (hereinafter for the purpose of this policy framework referred to as the "Head of Risk Management") has been vested with the task of facilitating the ERM process and to ensure that appropriate risk management procedures as detailed in the Risk Management framework are adopted and adhered to.

The Head of Risk Management will provide an update to the Risk Management committee of the Board on a periodic basis on key risks and the status of the risk mitigation actions.

The role of Risk Management function will include *inter-alia*: -

i. Facilitating discussions to review the Company's risk philosophy and the quantum of risk that the organization is willing to accept in pursuit of stakeholder value.

ii. Facilitating the establishment and development of an effective enterprise risk management framework
iii. Coordinate the effort of collating the status of risks mitigation actions against the key risks across business verticals and / or functions to deliver a consolidated portfolio view of risks to the internal Risk Steering committee as also to the Risk Management committee of the Board.
iv. Conduct internal risk review meetings including those with the risk steering committee, maintain risk registers, update the risk management policy, and suggest best practices for strengthening the overall enterprise risk management process.
v. Provide support in the review of *or* in the assessment of the effectiveness of risk management processes in identifying, assessing, and managing the Company's significant enterprise-wide risk exposures.

The risk management function will act as the interface between the internal Risk Steering committee as also the Risk Management committee of the Board.

d. Risk champions and Business functions:

The Business vertical and support function Heads of the Company are owners of the risks in the context of business objectives of their functions and are responsible for managing risks on various parameters as identified, and to ensure implementation of appropriate risk mitigation measures.

Risk champions are designated personnel identified from each of the business verticals / functions who will serve as point(s) of contact and are responsible for tracking the progress of risk mitigation action plans for key risks identified within the respective Business verticals / functions.

Periodic risk mitigation action updates as also status of the residual risks is to be collated and provided by the Risk champions from each of the Business verticals / functions and consolidated by the Head of Risk management for deliberation at the internal Risk Steering Committee and subsequently rolled up to the Risk Management Committee of the Board.

ii. Risk identification & mitigation:

Enterprise Risk Management (ERM) deals with risks and opportunities affecting value creation or preservation and is defined as *"a process, effected by the Board of Directors, Management and other personnel, (that is) applied in strategy setting and across the enterprise, (which is) designed to identify potential events that may affect the entity's business objectives, and manage risk to be within its risk appetite, (and) to provide reasonable assurance regarding the achievement of the organisation's objectives."*

The Business vertical and support functions of the Company are responsible to identify the risks including external and internal risk factors in the context of the defined business objectives.

While the purpose of this policy document is not to detail out the various risk identification techniques, the Risk Management function will facilitate periodic dialogues with the business stakeholders to identify key risks that can affect the attainment of strategic objectives. The techniques may include a combination of structured interviews, workshops or surveys as may be appropriate.

Risk mitigation is an ongoing process that is deployed by business managers during the normal course of business. Risk mitigation actions that could be deployed by the business risk owner can include any of the following courses of action based on the nature of the risk identified:

a. **Accept** – There may not be a specific course of action to mitigate the identified risk, and hence the residual risk will be accepted at the gross level of exposure. These will have to be monitored to review the nature of the impact of such risk events on the achievement of the strategic objectives of the enterprise.

b. **Avoid** – The organisation may decide to avoid taking the risk altogether.

c. **Transfer** – The risk may be transferred to a 3rd party (example – through Insurance)

d. **Treat** – The risk identified can be treated through specific internal control mechanisms / measures deployed to manage the risk.

e. **Terminate** – In specific cases, newer risks that may emerge may be terminated by the business if the costs of doing business post the incidence of such risk event far exceed the benefits arising from the opportunity identified (for example – where geopolitical risks emanate in a geographic region, it may warrant closure of the business in that geography).

iii. Risk management process:

The Enterprise Risk Management process will include *inter alia*:

a. Identification of business areas / domains subject to risk
b. Risk identification using a combination of techniques such as structured interviews, or risk workshops with key stakeholders to generate a comprehensive list of potential risk events that can potentially impact attainment of business objectives.
c. Prioritising risks that impact achievement of strategic business objectives based on the factor of likelihood (probability) and associated impact (consequence)
d. Undertake a structured Risk analysis with a view to identify underlying causes and sources of the potential risks and the trigger events that would lead to the occurrence of the risks, with a view to determine appropriate risk mitigation action plans.
e. Risk evaluation to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for implementation of treatment actions.
f. Recommendations to guide decisions on business risk issues.
g. Quarterly review and reporting with respect to closure of risks through Action taken reports.
h. Communication and consultation with external and internal stakeholders during all stages of the risk management process.
i. Review of strategic risks arising out of adverse external business conditions or lack of responsiveness to changes to the external environment.
j. Development of a comprehensive risk register to generate a comprehensive inventory of risks based on those events that might create, enhance, prevent, degrade, accelerate, or delay the achievement of objectives.

IV. Business Continuity Plan:

Business Continuity Plan ("BCP") ensures that personnel and assets are protected in the event of a High Impact & High Velocity risk is aimed to enable rapid response to address the consequence of such risks events when they materialize. Such risks may include but is not restricted to natural disasters— fire, flood, or weather-related events—and cyber-attacks.

BCP is an integral part of an organisation's enterprise-wide risk management strategy and is conceived in advance and involves input from key stakeholders and personnel.

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.*

V. Applicability:

This policy applies to FSN E Commerce Ventures Limited and its material subsidiaries *("Material subsidiary" shall mean a subsidiary whose income or net worth exceeds the thresholds as provided in the Listing Regulations).*

The Risk Management function of the Company is responsible for administration and compliance of this Policy.

VI. Limitation & Amendment:

In the event of any conflict between the provisions of the Risk Management policy and of the Companies Act or SEBI's Listing Regulations or any other statutory enactments or rules, the provisions of such Act or Listing Regulations or statutory enactments or rules shall prevail over this Policy.

Any subsequent amendment / modification in the Listing Regulations, Act and / or applicable laws in this regard shall automatically apply to this policy.

VII. Review:

This policy will be reviewed periodically (at least once in 2 years) by the Risk Management function as also the Risk Management committee of the Board to ensure it meets the requirements of legislation & the needs of organization.

VIII. Effective date:

This Policy is in force from the date of listing of equity shares of the Company on the stock exchanges. Amendments to the policy if any, will be effective from the date such amendments have been approved by the Risk Management Committee of the Board.

Document control:

Created by:	Internal Audit & Risk Management	March 2024
Reviewed by:	CFO, and MD & CEO	March 2024
Approved by:	Risk Management Committee of the Board of FSN E Commerce Ventures Limited	
Original policy effective from (date):	10th November 2021	
This version effective from (date)	8th May, 2024	
Current version number:	1.2	

Revision record sheet:

Sl. #	Version number	Date	Brief description of changes
1	1.1	10th November 2021	Original policy drafted, Approved by the Board of Directors
2	1.2	8th May, 2024	Update to the Risk Management Governance structure, defining Internal Risk Management governance processes; and terms of reference of the internal steering committee as also the risk champions. Also updated for consistency in language and construct of the flow of the Risk Management policy document.