


Policy Name		Risk Management Policy				
	Policy Owner	CFO	Policy ID	NA	Designed by	
	Function	Risk Management	Version No		Reviewed by	
	Sub-function	NA	Effective date		Policy Champion	


**FSN E-Commerce Ventures Limited**

**ERM Framework for Nykaa**

**NYKAA**

**Confidential and Privileged**

***This is an internal draft for discussion purposes only.***


Policy Name		Risk Management Policy				
 Your Beauty. Our Passion.	Policy Owner	CFO	Policy ID	NA	Designed by	
	Function	Risk Management	Version No		Reviewed by	
	Sub-function	NA	Effective date		Policy Champion	

Approval Matrix				
Name	Role	Function	Sign	Date

Document Change History				
Version No.	Effective Date	Change request by	Change made by	Change Type


Related Documents	
Document name	Process / Policy ID

Document Review Cycle				
#	Effective Date	Next review date	Policy Owner	

Policy Name		Risk Management Policy				
	Policy Owner	CFO	Policy ID	NA	Designed by	
	Function	Risk Management	Version No		Reviewed by	
	Sub-function	NA	Effective date		Policy Champion	


Policy Description	
<b>Objective</b>	<p>This policy is intended to ensure that an effective Risk Management program is established and implemented within FSN E-Commerce Ventures Limited (hereinafter referred to as company / organization) to identify enterprise level risk. This program will provide regular reports on:</p> <ol style="list-style-type: none"> <li>1. The performance of the ERM program, including any exceptions, to key stakeholders.</li> <li>2. The movement of identified Risk, to give an overview of the Risk Profile of the company as on a date.</li> </ol>
<b>Policy Summary</b>	<p>The policy contains the objectives of risk management, company's approach to risk management, and the risk organization structure for identification, management and reporting of risks. The policy also specifies the roles and responsibilities of key stakeholders and other key personnel of the company with regards to risk management.</p>

Members of Central Risk Office				
Name	Role	Function	Sign	Date

Policy Name		Risk Management Policy				
	Policy Owner	CFO	Policy ID	NA	Designed by	
	Function	Risk Management	Version No		Reviewed by	
	Sub-function	NA	Effective date		Policy Champion	

## TABLE OF CONTENTS

<b>1. ENTERPRISE RISK MANAGEMENT GOVERNANCE STRUCTURE .....</b>	<b>5</b>
<b>2. ROLES AND RESPONSIBILITIES .....</b>	<b>6</b>
2.1 BOARD OF DIRECTORS .....	6
2.2 AUDIT COMMITTEE .....	6
2.3 RISK MANAGEMENT COMMITTEE .....	6
2.4 CENTRAL RISK OFFICE .....	9
2.5 RISK AND MITIGATION OWNERS .....	11
2.6 INTERNAL AUDIT .....	13
<b>3. ERM CALENDAR .....</b>	<b>14</b>
<b>4. RISK ESCALATION AND CONTROL .....</b>	<b>14</b>
<b>5. RISK ASSESSMENT PARAMETERS .....</b>	<b>15</b>
<b>6. RISK REVIEWS .....</b>	<b>17</b>
<b>7. MANAGING MATERIALIZED RISKS .....</b>	<b>18</b>
<b>8. INCIDENT REPORTING / LOSS REPORTING .....</b>	<b>19</b>
8.1 DEFINITION OF AN INCIDENT .....	19
8.2 PURPOSE OF INCIDENT REPORTING .....	19
8.3 INCIDENT REPORTING PROCESS .....	19
8.4 SENIOR MANAGEMENT REPORTING AND ANALYZING INCIDENT .....	20
<b>9. KNOWLEDGE MANAGEMENT .....</b>	<b>20</b>
<b>10. ANNEXURES: .....</b>	<b>21</b>
1. ILLUSTRATIVE INCIDENTS .....	21

Policy Name		Risk Management Policy				
	Policy Owner	CFO	Policy ID	NA	Designed by	
	Function	Risk Management	Version No		Reviewed by	
	Sub-function	NA	Effective date		Policy Champion	

## 1. Enterprise Risk Management Governance Structure

The ERM Governance Structure identifies the key internal stakeholders responsible for creating, implementing, and sustaining ERM in the organization. The structure leverages existing organizational structure within the company in order to align individuals, teams, and departments with the objective of:


- Integrating ERM into the organization culture
- Facilitating and monitoring effective implementation of the ERM framework
- Ensuring that the ERM framework and its components are up to date
- Providing clarity over roles and responsibilities across the ERM processes

The risk governance structure is presented below, and the distinct roles and responsibilities are included in *Section 2*.



\*Functional owners

\*\*Functional owners / delegates

Policy Name		Risk Management Policy				
	Policy Owner	CFO	Policy ID	NA	Designed by	
	Function	Risk Management	Version No		Reviewed by	
	Sub-function	NA	Effective date		Policy Champion	

## 2. Roles and Responsibilities

### 2.1 Board of Directors

With respect to Risk Governance, the Board of Directors have the following responsibilities:

Area	Responsibility of BOD
Strategy planning	Determining the strategic direction of the organization
Risk Management	Establishing expectations with respect to Enterprise Risk Management
Risk Ownership	Owning risks of strategic importance impacting the company at an organizational level
Organization structure and roles & responsibilities	Endorsing the Enterprise Risk Management organization structure and authorizing roles and responsibilities for key stakeholders
Risk procedures / policy reviews	Review and approve risk management-related policies, procedures, and parameters
Continuous Monitoring of Risk	Reviewing the critical aspects that address material risks and strategic implications

Board may decide to execute these responsibilities through Risk Management Committee (RMC). The composition of RMC should be in accordance with clause 21 of Listing Obligations and Disclosure Requirements ('LODR').


### 2.2 Audit Committee

**Section 177(4) of the Companies Act, 2013** states that Every Audit Committee shall act in accordance with the terms of reference specified in writing by the Board which shall, inter alia, include, evaluation of internal financial controls and risk management systems.


### 2.3 Risk Management Committee

RMC will act as a sponsor for risk management in the organization and in doing so carry out the following responsibilities as approved by Board of Directors and as prescribed under Para C, Part D of Schedule II of SEBI LODR:

Area	Responsibility of RMC
Policy framework for risk management	Define policy and procedures for risk management. The policy shall include: <ul style="list-style-type: none"> <li>A <b>framework for identification</b> of internal and external risks</li> </ul>

Policy Name		Risk Management Policy				
	Policy Owner	CFO	Policy ID	NA	Designed by	
	Function	Risk Management	Version No		Reviewed by	
	Sub-function	NA	Effective date		Policy Champion	

Area	Responsibility of RMC
	<ul style="list-style-type: none"> <li><b>Measures for risk mitigation</b> including systems and processes for internal control of identified risks</li> <li><b>Recommend changes and submit to the risk appetite parameters/ risk profile</b> for approval of Board of Directors and Audit Committee</li> </ul>
Risk assessment, evaluation, escalation and mitigation	<ul style="list-style-type: none"> <li>Procedure of risk assessment to identify root causes/ sources for individual risks, assess the impact of risks on achievement of strategic and operational objectives and compare with risk thresholds/ appetite for appropriate response/ escalation</li> </ul> <p>With the objective of ensuring effective and timely identification of risk root causes, assessment of impact risks and risk prioritization</p>
Review of risk management policy	Periodically review the risk management policy at least once in two years, including by considering the changing industry dynamics and evolving complexity
Recommend change and submit	Recommend changes and submit to the risk appetite parameters/ risk profile for approval of Board of Directors and Audit Committee
Risk monitoring and assessment	Ensuring risk identification, assessment, prioritization, and profiling is done in an effective and timely manner and assessing significant breakdown in risk mitigation
Monitoring of risk response plans	Monitoring the progress of the risk response plans and strategies in collaboration with respective business functions in terms of response sufficiency, implementation status and effectiveness.
Escalation of key risks	Escalate key risk to Audit committee
Review risk response	Reviewing risk response strategies with respective business functions in terms of response sufficiency, implementation status and effectiveness
Tracking of new risks	Tracking the emergence of new risks and the progress of the risk response plans in collaboration with respective business functions
Compliance with risk limit/appetite	Ensuring compliance with risk limit/appetite established for the organization while tracking emergence of new risks
Risk management	Managing materialized risks by: <ul style="list-style-type: none"> <li>- assessing impact of the materialized risk event and advising remediations</li> <li>- coordinating with corporate communications/ Board of Directors and Audit Committee for external and internal communications</li> </ul>
Training	<b>Training:</b> Building risk awareness culture across the organization
Appointment, removal and remuneration of CRO	Consider the appointment, removal, and terms of remuneration of the company's chief risk officer (if any)

Policy Name		Risk Management Policy				
	Policy Owner	CFO	Policy ID	NA	Designed by	
	Function	Risk Management	Version No		Reviewed by	
	Sub-function	NA	Effective date		Policy Champion	

Area	Responsibility of RMC
CRO activity monitoring	Reviewing Central Risk Office (CRO) activities pertaining to Enterprise Risk Management
Resource allocation	Allocating adequate resources for treating critical risks and/ or risk events at the organization level
CRO support	Providing necessary support to the Company's Central Risk Office in performing risk management activities as envisaged
Communication of significant development	Communicating to the Central Risk Office for significant developments/ changes to business and other key business decisions
Liaising with BOD	Keep the Board of Directors informed about the nature and content of its discussions, recommendations, and actions to be taken
Correspondence with other Committees	Coordinating 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
Statutory compliances	Such terms of reference as may be prescribed under the Companies Act and SEBI Listing Regulations
Incorporating board suggestions	Attending to such other matters and functions as may be prescribed by the Board from time to time

### Constitution of RMC

As per Regulation 21, SEBI LODR Amendment (2021)

- The RMC shall have a minimum of three members with a majority of them being members of the board of directors
- The composition of RMC shall include at least one independent director

### Number of meetings and quorum :

- The RMC shall meet at least twice in a year.
- The quorum shall be either two members or one- third of the committee members, whichever is higher, including at least one member of the board of directors in attendance


### Maximum gap between meetings:

The meetings of the RMC shall be conducted in such a manner that on a continuous basis, not more than 180 days shall elapse between any two consecutive meetings.

### Disclosure in annual report about RMC:

Listed companies to disclose the following about RMC in the annual report:

- Brief description of terms of reference

Policy Name		Risk Management Policy				
	Policy Owner	CFO	Policy ID	NA	Designed by	
	Function	Risk Management	Version No		Reviewed by	
	Sub-function	NA	Effective date		Policy Champion	

- Composition, name of members and chairperson
- Meetings and attendance during the year

**Core Committee (Majority member to be from board of directors) :**

- Independent Director
- Independent Director
- Managing Director
- Whole Time Director & Business / Functional Heads (invited on need basis)

**Consultation**

- Head of Internal Audit


**Convener**

- CRO


## 2.4 Central Risk Office

The role of the Central Risk Office will be to facilitate development, implementation and monitoring of risk management across the organization. The central risk office may be headed by the Chief Risk Officer (if appointed) or by any other person as may be decided by the Risk management committee.

Area	Responsibility of CRO
Program Leadership	Providing overall leadership to ERM process in line with directions of the Board of Directors and Audit Committee
Program Ownership	Communicating the ERM and organization structure. Developing and assuming ownership of the risk management policy, framework, and process
ERM framework	Managing implementation of the ERM framework
Risk appetite	Providing necessary information to facilitate definition of risk appetite at the business line/ function, entity, and organization level
Reporting / Consultation	Liaising with Risk Management Committee at various levels for deploying the ERM process, reviewing enhancing and updating ERM process
Deviation management	Reviewing significant deviations from the ERM framework or other procedures and reporting them to Board of Directors, Audit Committee and Management Committee as appropriate
Review procedures	Assisting with implementation of procedures for proactive review of risks for projects, transactions, new businesses, etc. and assisting BOD and Audit

Policy Name		Risk Management Policy				
	Policy Owner	CFO	Policy ID	NA	Designed by	
	Function	Risk Management	Version No		Reviewed by	
	Sub-function	NA	Effective date		Policy Champion	

Area	Responsibility of CRO
	Committee for effecting changes to the risk management organization and process
Monitoring trends	Monitoring external trends and factors that may have significant impact on the risk profile of the organization and communicating the information to all key stakeholders
Reporting	Co-ordinating risk reporting to the Risk Management Committee, Board, and the Audit Committee
Risk Management	Co-ordinating with and HO functions on activities which rely on the risk management for risk related inputs
Risk Identification	Assist in Risk Identification. Identification of impact assessment and risk prioritization
Continuous monitoring and updation	Implementation of procedures for risk assessment including proactive review of risks, monitoring of external trends that impact the risk profile of the organization and coordinating risk reporting. Coordinating with HO Risk Owners for new risks identified or changes to risks
Maintenance of register and risk profile	<p>Maintain and review the risk registers and the risk response plan tracker.</p> <p>Following are the critical characteristics of a SMART risk profile:</p> <ul style="list-style-type: none"> <li>• Specific: The plan should be clear and not general in nature</li> <li>• Measurable: The output of the plan should be easy to 'quantify' to monitor its performance</li> <li>• Achievable: The plan should be attainable by the existing and available resources</li> <li>• Relevant: The plan should be focused towards mitigating the risk identified</li> <li>• Time bound: The plan should be executed within a period to contain any adversity from the risk</li> </ul>
Risk response plans	Providing input and feedback on proposed risk response plans and initiatives
Monitoring risk response plans	Monitoring progress of implementation of risk response plans and strategies. And reporting mitigation plans and significant breakdown in mitigation to relevant stakeholders and compliance with risk appetite
Periodic risk reviews	Ensuring that risk reviews are carried out on a periodic basis in order to maintain continuity of the enterprise risk management process

Policy Name		Risk Management Policy				
	Policy Owner	CFO	Policy ID	NA	Designed by	
	Function	Risk Management	Version No		Reviewed by	
	Sub-function	NA	Effective date		Policy Champion	

Area	Responsibility of CRO
Risk and mitigation plan reporting	Preparing and communicating risk reports with risk mitigation measures to relevant stakeholders
Incident database	Updating the loss event / incident database based on information on materialized risks from HO Risk Owners risk owners to monitor and report incidents and materialized risk
Risk escalation	Escalating risk to appropriate level
Training	Training and collaborating with the business lines and divisions in executing ERM framework on a regular basis to aid management in decision making
Promote culture	Promoting risk management culture through trainings, reporting and other internal communications
Training calendar	Developing an annual risk management training calendar to ensure that individuals engaged in risk management are: <ol style="list-style-type: none"> <li>1. Developed with appropriate risk management skills and competencies</li> <li>2. Developing the analytical systems and data management capabilities to support the ERM program</li> </ol>


## 2.5 Risk and mitigation Owners

The **Business vertical and support function Heads** of the Company are owners of the risk of their functions and are responsible for managing risk on various parameters and ensure implementation of appropriate risk mitigation measures. CRO of the Company is responsible for administration and compliance of this Policy

All the business functions and units of the company have a primary responsibility for managing risk on a day-to-day basis. The role of risk owner and mitigation owner is as follows:

### Risk Owner


Area	Responsibility of Risk Owner
Risk policy management	Introduction and promotion of risk management policy, procedure and processes and culture
Incorporation of risk management	Ensuring that risk management is incorporated in the business decision making process and assuming overall responsibility for mitigating individual risk
Risk mitigation	Assuming overall responsibility for mitigating the individual risk, that is overall management of the risk response as agreed in the risk profile

Policy Name		Risk Management Policy				
	Policy Owner	CFO	Policy ID	NA	Designed by	
	Function	Risk Management	Version No		Reviewed by	
	Sub-function	NA	Effective date		Policy Champion	

Area	Responsibility of Risk Owner
Risk assignment	Ensuring responsibility and actions are assigned to appropriate mitigation owners against agreed upon risk response plans and develop training calendar
Monitoring risk plans	Monitoring the progress of the risk treatment plans against the agreed milestones and evaluating the impact of the mitigation plan
Periodic risk evaluation against threshold	Periodically evaluating the impact of the mitigation plan on the risk, against the risk threshold level, risk evaluation/ prioritization parameters, and the subsequent impact on the residual risk
Reporting to CRO Office	Timely escalating of challenges, concerns or unforeseen developments pertaining to the risk to the CROs office who shall then evaluate the situation and accordingly report to the RMC and Board
Risk reporting	Proactively reporting significant breakdowns in risk mitigation measures and actions to prevent their recurrence
Identify and reporting new risks to CRO Office	Identifying new emerging risks periodically and report to the CROs office (for assessment, prioritization, and response planning)
Risk escalation and status	Risk escalating to the CRO office and reporting to the CROs office on the status of the risk and its treatment plan
Reporting significant breakdown in risk mitigation measures	Reporting significant breakdowns in risk mitigation measures and actions to prevent their recurrence

### Mitigation Owner

Area	Responsibility of Mitigation Owner
Liaising with risk owners	Working with risk owners to implement agreed mitigation action plans
Mitigation management	Assuming the role of a SPOC (single point of contact) for managing the mitigation of an individual risk as identified in the risk register
Reporting	Periodically updating the risk owner on status of execution along with relevant KPI's
	Timely escalating challenges, concerns, or unforeseen developments to risk owner
	Proactively reporting significant breakdowns in risk mitigation measures and actions to prevent their recurrence

Policy Name		Risk Management Policy				
	Policy Owner	CFO	Policy ID	NA	Designed by	
	Function	Risk Management	Version No		Reviewed by	
	Sub-function	NA	Effective date		Policy Champion	

## 2.6 Internal Audit

Internal Audit (IA) provides independent assurance of the risk management system and the processes supporting it. Its role is essentially to review the overall effectiveness of the risk management measures and controls. The position of Internal Audit within the company also puts it in a good position to assist the Board of Directors/ Audit Committee in their monitoring function and to play an integral part in the promotion of risk management generally.

Internal Audit is specifically responsible for:


- Aligning internal audit plans to risk profiles to ensure that risk management activities for all key risks are covered as a part of the internal audit process
- Identifying and putting emphasis on the potential impact of weaknesses in the ERM system.
- Supporting the risk management process in all business functions by providing advice about risk management standards and best-practice procedures.

In order to enable Internal Audit to effectively leverage the ERM output and vice versa:

- ERM department shall share the list of risks identified on a periodic basis or as requested by IA. Internal audit may use this information as an input for developing a risk-based Audit plan

IA shall share the respective audit reports with the ERM function on a need basis. The ERM function may use this information as an input for risk treatment plans.

**Refer Annexure 2 for Roles and Responsibility Matrix**

Policy Name		Risk Management Policy				
	Policy Owner	CFO	Policy ID	NA	Designed by	
	Function	Risk Management	Version No		Reviewed by	
	Sub-function	NA	Effective date		Policy Champion	

### 3. ERM Calendar

#	Activities	Resp.	Frequency
1	<b>Assessment and approval of companies' Risk Appetite</b> (including risk assessment parameters)	RMC	Annual
2	<b>Reevaluate top enterprise risks</b> of strategic impact	RMC & CRO Office	Annual
3	Review, update (where necessary) and communicate the <b>ERM policy</b>	RMC & CRO Office	once in 2 years
4	<b>Inputs on risk from CRO Office</b> in preparation of AOP & <b>Risk identification (new risk)/ Risk Validation (existing risk)</b> based on the Annual Operating Plans at company	CRO Office & Business	Annual
5	<b>Risk identification</b> based on 'Signals of Change' (/ Risk Drivers)	CRO Office	Ongoing
6	<b>Inputs to Audit Committee</b> for consideration in development of IA plan	CRO Office & IA	Annual
7	<b>Risk Assessment</b> for calculating ' <b>Gross or Inherent Risk</b> ' and ' <b>Residual Risk</b> '	CRO Office	Ongoing
8	Review and update the <b>Risk Register</b> (including mitigation plans and new risks)	CRO Office	Ongoing
9	<b>Monitor and update / create Risk Profiles for material risks</b> (including mitigation plans)		Half yearly
10	<b>Monitor Risk Indicators</b> agreed with the Risk/ Mitigation Owners	CRO Office	Half yearly
11	Updation of the <b>Loss Event Database</b>	CRO Office	Ongoing
12	<b>Risk Reporting</b> to the RMC	CRO Office	At least once in 180 days
13	<b>Risk Reporting</b> to the AC/ BOD	CRO Office	Audit committee scheduled after RMC


### 4. Risk Escalation and Control

A critical element of ERM is an effective system of escalation which ensures that specific issues are promptly communicated to relevant authorities. The escalation process links the results of risk assessment with the risk organization structure and responsibility levels. Section 2 and Section 3 – Enterprise Risk Organization Structure and Roles and Responsibilities establishes clear reporting lines and defines responsibilities of the various levels of the ERM structure.

Risk escalation may stem from one or more of the following:


- Identification of new risks at business line and entity level
- Change in impact/ likelihood of identified risks causing a change in the risk evaluation
- Unforeseen contingencies

Risk control refers to policies and procedures that help ensure that the risk responses identified as determined by the risk owners are carried out.


Policy Name		Risk Management Policy				
	Policy Owner	CFO	Policy ID	NA	Designed by	
	Function	Risk Management	Version No		Reviewed by	
	Sub-function	NA	Effective date		Policy Champion	

## 5. Risk Assessment Parameters

Ref.	Scale	Calculation	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
1. Financial Parameters							
1.1	Financial - Potential impact on Revenue	% of ‘Last 3 years Total Revenue’	Less than or equal to 0.1%	More than 0.1% but less than or equal to 0.25%	More than 0.25% but less than or equal to 0.5%	More than 0.5% but less than or equal to 1%	More than 1%
		Absolute value (whichever is lesser)	< INR 1.5 Cr	INR 1.5 Cr – INR 5 Cr	INR 5 Cr – INR 15 Cr	INR 15 Cr – INR 25 Cr	> INR 25 Cr
1.2	Financial - Potential impact on Profitability	% of ‘Last 3 years EBITDA’	Less than or equal to 0.5% of EBITDA	More than 0.5% but less than or equal to 1.5% of EBITDA	More than 1.5% but less than or equal to 3% of EBITDA	More than 3 % but less than or equal to 5% of EBITDA	More than 5% of EBITDA
		Absolute value (whichever is lesser)	< INR 12 lakhs	INR 12 lakhs – INR 40 lakhs	INR 40 lakhs – INR 80 lakhs	INR 80 lakhs – INR 1.25 cr	> INR 1.25 Cr
2. Regulatory Parameters							
2.1	Potential financial penalties from regulator	Regulatory and legal non compliances resulting in a notice/ warning from the regulator	Regulatory and legal non compliances with potential financial penalties upto INR 5 Lacs	Regulatory and legal non compliances with potential imprisonment and/or financial penalties between INR 5 Lacs and INR 50 Lacs	Regulatory and legal non compliances with potential imprisonment and/or financial penalties between INR 50 Lacs to INR 1 Cr	Regulatory and legal non compliances with potential imprisonment and/or financial penalties greater than INR 1 Cr	Potential financial penalties from regulator
3. Reputation Parameters							

Policy Name		Risk Management Policy				
	Policy Owner	CFO	Policy ID	NA	Designed by	
	Function	Risk Management	Version No		Reviewed by	
	Sub-function	NA	Effective date		Policy Champion	

Ref.	Scale	Calculation	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
3.1	Brand Image - Potential impact on brand image	Qualitative impact (Reputational)	Impact on brand image but can be prevented through immediate corrective action	Impact on brand image but contained within the organization within a specific circle	Reputational loss contained within the organization but with a reach across multiple circles	Reputational loss at circle level, with mass reach (i.e., media and public)	Reputational loss at national/ international level/group level
3.2	Attrition - Potential impact on operations of company due to Attritions	Qualitative Impact (Critical Employees are CEO/COO and HoDs, or any employee who has been identified as critical by virtue of specific knowledge/skills Key Employees - Who have been rated as exceptional performers for a continuous period of 2 years	a) Limited attrition of non-key employees – can be managed through normal recruitment	a) Moderate attrition of non-key employees - may require focused effort on recruitment	a) Extensive attrition of non-key employees - may require focused effort on recruitment b) Loss of 20 key employees	a) Loss of > 20 key employees b) Loss of 3 critical employee along with his/her entire team	a) Loss of > 3 critical employees along with his/her entire team
3.3	Non-Financial - Potential impact on the control environment and relationships (internal and external)	Qualitative and Quantitative Impact	a) No risk of litigation b) Disruption in relation with 10% of non-strategic vendor c) Impacts < 5% of the customer base d) Geopolitical situation with no impact	a) Arbitration with financial penalty as mentioned in 2.1 b) Disruption in relation with 20% of non-strategic vendor c) Impacts 5% to 10% of the customer base d) Geopolitical	a) Court litigation with possible penalty as mentioned in 2.1 b) Disruption in relation with 30% of non-strategic vendor c) Impacts 10% to 20% of the customer base d) Geopolitical	a) Court litigation with possible penalty as mentioned in 2.1 b) Disruption in relation with 5% of strategic vendor c) Impacts 20% to 30% of the customer base d) Geopolitical situation with long term closure of operations	a) Court litigation with possible penalty as mentioned in 2.1 b) Disruption in relation with 10% of strategic vendor c) Impacts > 30% of the customer base d) Geopolitical situation with

Policy Name		Risk Management Policy				
	Policy Owner	CFO	Policy ID	NA	Designed by	
	Function	Risk Management	Version No		Reviewed by	
	Sub-function	NA	Effective date		Policy Champion	

Ref.	Scale	Calculation	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
				situation with minor impact	situation with temporary closure of operations		permanent closure of operations

## 6. Risk Reviews

Periodic risk monitoring, review and reporting are critical components for the success of the ERM process.


The intent of monitoring and reviewing risks and their respective response plans is to:

1. Analyze and track events, changes, trends which effect identified risks
2. Assess the impact of such changes to risk assessment and evaluation
3. Assess the impact of such changes on response plans

**Risk monitoring** should be conducted by each business line and function on a monthly basis, for identified risks, in order to track the status of response plans and to consequently update changes to risk profiles.

**Risk reviews** involves re-examination of the risk register, risk assessment and risk response including the risk profiles. The risk review is conducted by the management to monitor the effectiveness of the ERM framework. Risk reviews entail updation of the risk registers with updated risk assessment, new/ emerging risks, and the related responses and profiling. The risk reviews should be carried out on a yearly basis and updated in the risk report.

The Central Risk Office shall initiate and assist the risk monitoring and risk review process. However, the responsibility of updation of the risk register, risk assessment and risk response, including risk profiles, lies with the respective risk and process owners.

Policy Name		Risk Management Policy				
	Policy Owner	CFO	Policy ID	NA	Designed by	
	Function	Risk Management	Version No		Reviewed by	
	Sub-function	NA	Effective date		Policy Champion	

## 7. Managing Materialized Risks

It is necessary to have a crisis/ incident response plan for timely and effective management of an event of a risk materializing. The incident management plan is a set of well-coordinated actions aimed at preparing and responding to unpredictable events with adverse consequences. The intention of this plan is to preserve the confidence of internal and external stakeholders in companies risk readiness for potentially adverse events.


The crisis management plan should detail out the following:

1. The situations for which action plans shall be invoked
2. The manner in which such plans shall be actioned
3. The individuals/ departments involved in such planning and execution

Tracking data pertaining to materialized risks is an essential input to the development and functioning of ERM. Such data is crucial for effective risk reviews based on actual historical experience.

The data pertaining to materialized risks shall be captured in a “Loss event database”. Typical loss events can include (but may not be restricted to):

4. Unforeseen political or regulatory changes
5. Damage/ loss of critical network assets resulting in network outage or deteriorating quality
6. Environment, Health and Safety incidents
7. Fraud – internal and external
8. Loss of key customers/ vendors/ alliances
9. Technology/ system failures & Cyber-attacks including Hacking

Policy Name		Risk Management Policy				
	Policy Owner	CFO	Policy ID	NA	Designed by	
	Function	Risk Management	Version No		Reviewed by	
	Sub-function	NA	Effective date		Policy Champion	

## 8. Incident Reporting / Loss Reporting

### 8.1 Definition of an incident

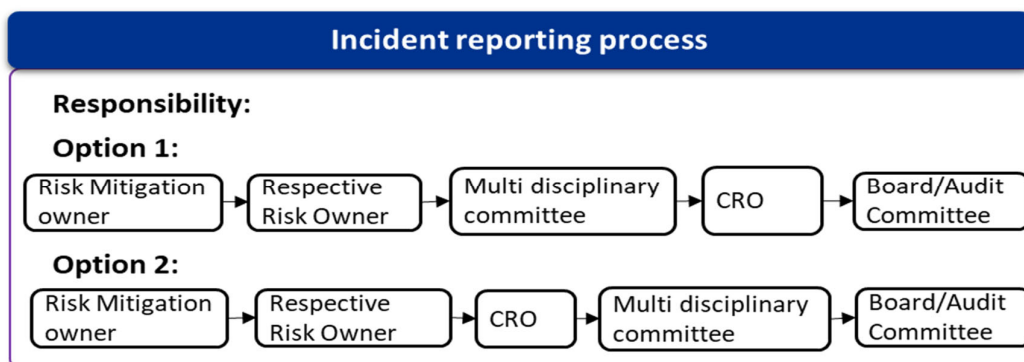
Incident can be defined as an instance of something happening, an event or occurrence. Incident can be an instance of employee injury, property damage, improper conduct, security breach, fraud, or other reasons. For the organization incident which falls within the parameters. can be termed as incident meant to be reported or anything else which the Risk owners or unit heads deem fit. *(Refer Annexure 1 for list of incidents)*


### 8.2 Purpose of incident reporting

Incident reports are one of the most important forms of documentation for a corporation to employ in their day-to-day operations for a multitude of reasons. Whether reporting an instance of employee injury, property damage, improper conduct, security breach, fraud, or other reasons, it is increasingly important for a company to keep an effective Incident reporting process. Some of the key benefits include:

1. Provide valuable feedback to risk assessments. One of the primary challenges is that risks may be assessed on an overly optimistic basis. Having effective Incident reporting enables risks to be objectively tracked for occurrence and impact.
2. Avoiding unnecessary fines and claims where there is appropriate documentation in place, along with mitigation plans. This is particularly important if incident reporting is regulated, such as in the case of Medical Care providers.
3. Captures intelligence for Prevention Strategies – this includes identifying gaps in the existing business processes and provide opportunities for improvements in efficiency and quality.

### 8.3 Incident reporting process



Policy Name		Risk Management Policy				
	Policy Owner	CFO	Policy ID	NA	Designed by	
	Function	Risk Management	Version No		Reviewed by	
	Sub-function	NA	Effective date		Policy Champion	

#### 8.4 Senior management reporting and analyzing incident

Senior management i.e., CRO office and the team identified as senior management for this purpose shall discuss and deliberate on the incident and action to be taken to mitigate the risk. This action to be taken shall be proposed to the board which shall then either approve the action or suggest alternate action after analyzing the incident

### 9. Knowledge Management

This section seeks to provide specific reference to the ERM practitioners within the company on ERM documentation and document retention.

#### Documentation


The following documents are generated during the course of the ERM exercise.

Document	Description	Owner	Periodicity of review
Risk register	Record/ log of information about identified risks	Central Risk Office	Ongoing
Risk report	A report/ form of communication intended to inform particular stakeholders of the <b>current state of key risks and its mitigation</b> . It is represented by a "Heat Map" where key risks are plotted and is supported by the detailed risk profiles	Risk Management Committee	Quarterly
Risk profile	Detailed description of a risk including current risk response, and details of management action plans for further treatment including responsibilities and timelines	Risk owners	Ongoing
Loss event database/ Incident reporting	Whenever a loss event occurs, its severity and date of occurrence would be entered into a <i>loss event database</i> and attributed to the business function/ entity it affected/ it belonged to	Risk Management Committee	Event driven i.e., as, and when the loss event occurs

#### ERM Framework Management

The ERM framework is owned by the Central Risk Office. Changes to the document need to be processed through the CROs office and require the consensus of the Board of Directors and Audit Committee.

The Central Risk Office shall ensure that updates to the framework are communicated across the organization and shall also be responsible for promoting risk awareness across the company. The Central Risk Office may use tools, workshops, newsletters, formal training sessions, and undertake other initiatives as deemed required for this purpose.

Policy Name		Risk Management Policy			
	Policy Owner	CFO	Policy ID	NA	Designed by
	Function	Risk Management	Version No		Reviewed by
	Sub-function	NA	Effective date		Policy Champion

### Record retention


For the purpose of ensuring traceability of ERM activities, documentation shall be maintained in physical or electronic form and retained for period mandated by law for financial data under companies and/ or income tax act. Records, both physical and electronic, at the organization level shall be maintained by the Central Risk Office on behalf of the Audit Committee and Board of Directors.

However, those at the business unit and function shall be maintained by individual BU and function representatives designated for this purpose.


## 10. ANNEXURES:

### 1. Illustrative Incidents


Department	Incident	Threshold
Retail / WH operations	Any Statutory notice / Panchama by local authorities (Police or municipal, labor officer, legal metrology, customs, etc.) and reporting of any noncompliance.	All
	Incident at the store / WH of such as fire, theft, or any major incident (Act of God) having risk to the company's assets such as cash, stock, etc.	All
	Delivery executive absconds with cash collected from customers	All
	Any notice with the landlords with regards to financial terms or possession of property under contrail lease / license that may result in business disruption	All
	Changes to the local policies impacting operations / infrastructure leading to business disruptions	All
	Customer complaints for damaged products / poor quality products purchased	Above KPIs
	Significant delay in completion of new projects (warehouse, Stores roll out etc.)	Above KPIs
Customer Experience	Negative sentiments/trolls / adverse social media reporting	All major issues
	Customer Complaints for DND/cold calling /calls for schemes / awards	All major issues
	Customer complaints for fake/damaged products ordered online / through store / fraud complaints	All major issues
	Significant Customer complaints / notices to company due to adverse reaction on using Nykaa's owned brand products or delivery issues on account of any e-commerce order servicing	Above KPIs
Technology and Info Security	E-commerce platform is not accessible due to downtime / server failure	Failure time in excess of xx hours
	Major system / support downtime / server failure beyond defined uptime thresholds	All
	Theft of business sensitive critical data /customer personal information (PII/ SPI)	Major breaches
	Cyber incidents such as leaks and breaches / Hacking/cyber-attacks/phishing / malware attacks / virus attacks / password or data thefts / DDoS on Nykaa's platforms and systems	Major breaches

Policy Name		Risk Management Policy			
	Policy Owner	CFO	Policy ID	NA	Designed by
	Function	Risk Management	Version No		Reviewed by
	Sub-function	NA	Effective date		Policy Champion

	Failure on account of business partners to protect customer personal information	Major breaches
	Major data backup failure / DRP failure	Major breaches
	Major technology implementation failure	Major breaches
	Any notices under information technology Act or any other regulation driving technology including RBI guideline to be complied by service partners such as custodian wallet / gift card providers / Nodal accounts	Any
	Frequent failure / unavailability of programs/ platforms / bugs in codes used for system development	As per KPI
	Fake website with a name or logo similar to Nykaa	Summary
	Incident of Fake / banned / illegal / infringed products listed on website	All
Admin and HR	Sudden (High) Attrition rate of experienced/senior staff/KMP / critical functions beyond standards as per quarterly report	Above KPI
	POSH Complaints reported	(To be managed separately by NRC)
	Business sensitive information leakage by Employees / third party staff / business partners	AS per the SOP
	Business reputation or financial loss reported by employee or identified through any sources for incident of frauds / misconduct / negligence or noncompliance to Code of conduct by any Employee	All
	Significant incident in the online social media by employees impacting Nykaa brand / reputation	All
	Non-compliance / delay in compliances with labor rules by contractors impacting principal employment	All
Finance	Restatement of published results	Above KPI
	Qualification of opinions by auditors of the company	All
	Duplicate payment / Wrong payments / in appropriate financial outflow impacting P&L	Above KPI
	Encashment of any bank guarantees issued by the company	Above KPI
	Depreciation of Indian rupee against foreign currency / High uncovered foreign exchange liability	Above KPI
	Exceptional collection shortage beyond average norms	Above KPI
	Default in compliance to loan covenants / delay / non servicing of loans	Above KPI
	Bankruptcy for Key customers	Above KPI
	Notice, visits, inspection by officials leading to payment of duties, liabilities, interest, tax, penalties, or legal notices	All
	Raid by tax or any other regulatory authority at a specific place / across the organization	All
Investments / M&A	Inability to raise fresh capital / funds by the company	Any major deviation
	Expected financial results not achieved post-merger / acquisition	Any major deviation


Policy Name		Risk Management Policy			
	Policy Owner	CFO	Policy ID	NA	Designed by
	Function	Risk Management	Version No		Reviewed by
	Sub-function	NA	Effective date		Policy Champion

	Investment provided for / closed (identified as bad investment)	Any major deviation
Legal & Regulatory	Infringement of brand / trademarks / Patent and copyrights by third party or alleged Infringement of brand / trademarks / Patent by Nykaa owned brands	All
	Whistle blower complaints against employee's / vendors of the company	All
	Incident of non-compliance (wrt environmental/labor/regulatory compliance etc.) including at third party operation	All
	Reporting of Insider trading	All
	Any reported non-compliance / delay in compliances with both domestic and international laws	All
	Legal Notice / Litigation / court case filed against the company by customer / vendor / marketplace sellers / public at large	All
Supply chain and Order management for marketplace / online sales	Significant Delays in Indian / Imported supplies from vendors / sole supply vendors vis a vis agreed timelines including for private label brands	AS per agreed KPIs/ Thresholds
	Trends in % of inactive customers	AS per agreed KPIs/ Thresholds
	Unreconciled / disputes in receivables from logistic partners	AS per agreed KPIs/ Thresholds
	Discontinuation of the brand for poor performance / disputes with key brands / supply issues etc./ Disruption in supply with regards to key strategic vendors	AS per agreed KPIs/ Thresholds
	Significant (% in excess of KPI) Shrinkage / shortage in inventory at warehouse during cycle count / periodic count	AS per agreed KPIs/ Thresholds
	Muted performance / low contribution of private labels viz a viz overall business of the company	AS per agreed KPIs/ Thresholds
	High nonmoving / slow moving / near expiry stock / increased inventory provisioning expense in a quarter	AS per agreed KPIs/ Thresholds
	No SKUs under Stockout / not available for sale and corresponding GMV trend	AS per agreed KPIs/ Thresholds
	Returns or Order cancellations in excess of defined limits / KPIs	AS per agreed KPIs/ Thresholds
	Major Breakdown in the order fulfillment beyond standard time. This can happen for certain geographies. Reason could be issues pertaining to fulfillment operations, or tech issues or due to any such issues with service provider / partners	AS per agreed KPIs/ Thresholds
Global	Any change in the statutory rules, regulations, policies potentially leading to business disruption	All
	Adverse geopolitical situations both domestic and international	All
	Occurrence of natural calamities or epidemic breakout disrupting operations	All
	Changes to foreign policy related to exporting/ importing countries	All

Policy Name		Risk Management Policy				
	Policy Owner	CFO	Policy ID	NA	Designed by	
	Function	Risk Management	Version No		Reviewed by	
	Sub-function	NA	Effective date		Policy Champion	

## 2. Roles and responsibility (summary)


#	Activity	Details	Board	RMC	CRO Office	Risk owners	Mitigation Owners
A	Strategic Risk Planning	Strategic direction for the organization	Determining				
		Risks of strategic importance	Owning				
		R&R for key stakeholders	Authorizing				
		Drive nature and content of its discussions at board		Communicating			
		Recommend activities between various sub-committees		Coordinating			
B	ERM Charter and policy	Enterprise Risk Management - Establishing expectations	Endorsing	Defining, Recommending	Communicating		
		Organization structure	Endorsing	Defining, Recommending	Communicating		
		Risk management policy, procedures, and processes	Reviewing, Approving	Defining, Recommending	Implementation, Ownership, Enhancing	Introduction, Promotion, Incorporation	
		Changes to the risk management policy, procedures, and processes	Reviewing, Approving	Defining, Recommending	Implementation, Ownership, Enhancing	Introducing, Promoting, Incorporating	
		Appointment of the Chief Risk Officer		Considering, Authorizing			
		Risk management culture			Owning	Promoting	
		Training calendar			Assisting in development	Developing	
		Deviation from ERM framework to Board			Reporting		
C	Company Risk Profile	Risk appetite parameters/ Risk profile	Approval	Recommending			
		Periodic review of Risk profile	Approval	Recommending		Assessing	

Policy Name		Risk Management Policy				
 Your Beauty. Our Passion.	Policy Owner	CFO	Policy ID	NA	Designed by	
	Function	Risk Management	Version No		Reviewed by	
	Sub-function	NA	Effective date		Policy Champion	

#	Activity	Details	Board	RMC	CRO Office	Risk owners	Mitigation Owners
		Compliance with risk limit/appetite		Ensuring	Monitoring	Reporting	
D	Risk Identification	Emerging risks Identification			Assisting	Owning	
		Periodic review of Risk identified				Assessing and Reporting	
		Impact assessment		Approving	Identifying		
		Risk prioritization		Approving	Identifying		
		Escalate risk to appropriate level		Monitoring	Monitoring, Reporting		
E	Risk Mitigation Plan	Assignment of mitigation plans / Actions to mitigation owner				Assigning	Owning
		Response plans / mitigation plans	Reviewing*	Assessing	Monitoring, Reporting	Owning	Implementing
		(*Only critical) Reporting Progress of the risk response plans		Reviewing	Monitoring, Reporting	Owning	Implementing
		Significant breakdowns in Risk mitigation		Assessing	Monitoring, Reporting	Owning	Reporting
F	Risk Assessment	Procedures for risk assessment		Defining	Implementation		
		Risk Register Preparation and maintenance			Implementation		
		Periodic risk reviews			Implementation		
G	Incident Reporting and Materialized Risk	Incidents Reporting		Assessing	Monitoring, Reporting	Owning	
		Managing materialized risks		Assessing	Monitoring, Reporting	Owning	Managing

### 3. Abbreviations

Terminology & Abbreviations		
S. No.	Short form	Full form
1	BU	Business Unit
2	CFO	Chief Financial Officer

Policy Name		Risk Management Policy				
	Policy Owner	CFO	Policy ID	NA	Designed by	
	Function	Risk Management	Version No		Reviewed by	
	Sub-function	NA	Effective date		Policy Champion	

Terminology & Abbreviations		
3	CRO	Chief Risk Officer
4	ERM	Enterprise Risk Management
5	IA	Internal Audit
6	MD	Managing Director
7	PESTLE	Political, Economic, Social, Technological, Legal and Environmental
<b>S. No.</b>	<b>Short form</b>	<b>Full form</b>
8	NGT	National Green Tribunal
9	RMC	Risk Management Committee
10	LODR	Listing Obligations and Disclosure Requirements

*NYKAA*