Sanofi India Limited

Risk Management Policy and Framework

Board approval date V2: 3rd November, 2022
Board approval date V1: 26th October, 2021
Effective date: 28th February, 2019

Contents

1. PURPOSE AND OBJECTIVES

Sanofi India Limited ("Sanofi") is operating in a volatile, uncertain, complex and ambiguous environment, and risk is inherent to its activity. Risks which may impact Sanofi's ability to achieve its strategy, objectives and results, must be identified, assessed, and managed in a timely, efficient and proactive and in a systematic manner.

Enterprise Risk Management (ERM) is defined as the culture, capabilities and practices, integrated with strategy-setting and performance that organizations rely on to manage risk in creating, preserving and realizing value.

Enterprise Risk Management (ERM) enhances financial health, sustenance and growth of a business and create value for stakeholders. To effectively embed the ERM process in culture and business processes, Sanofi has laid down an ERM Policy. In order to effectively implement and ensure adherence with the ERM Policy, this ERM policy has been developed. This document outlines the details of ERM principles, standards, and objectives along with associated procedures to be followed by all concerned stakeholders.

The key objectives of this policy are to help management in:

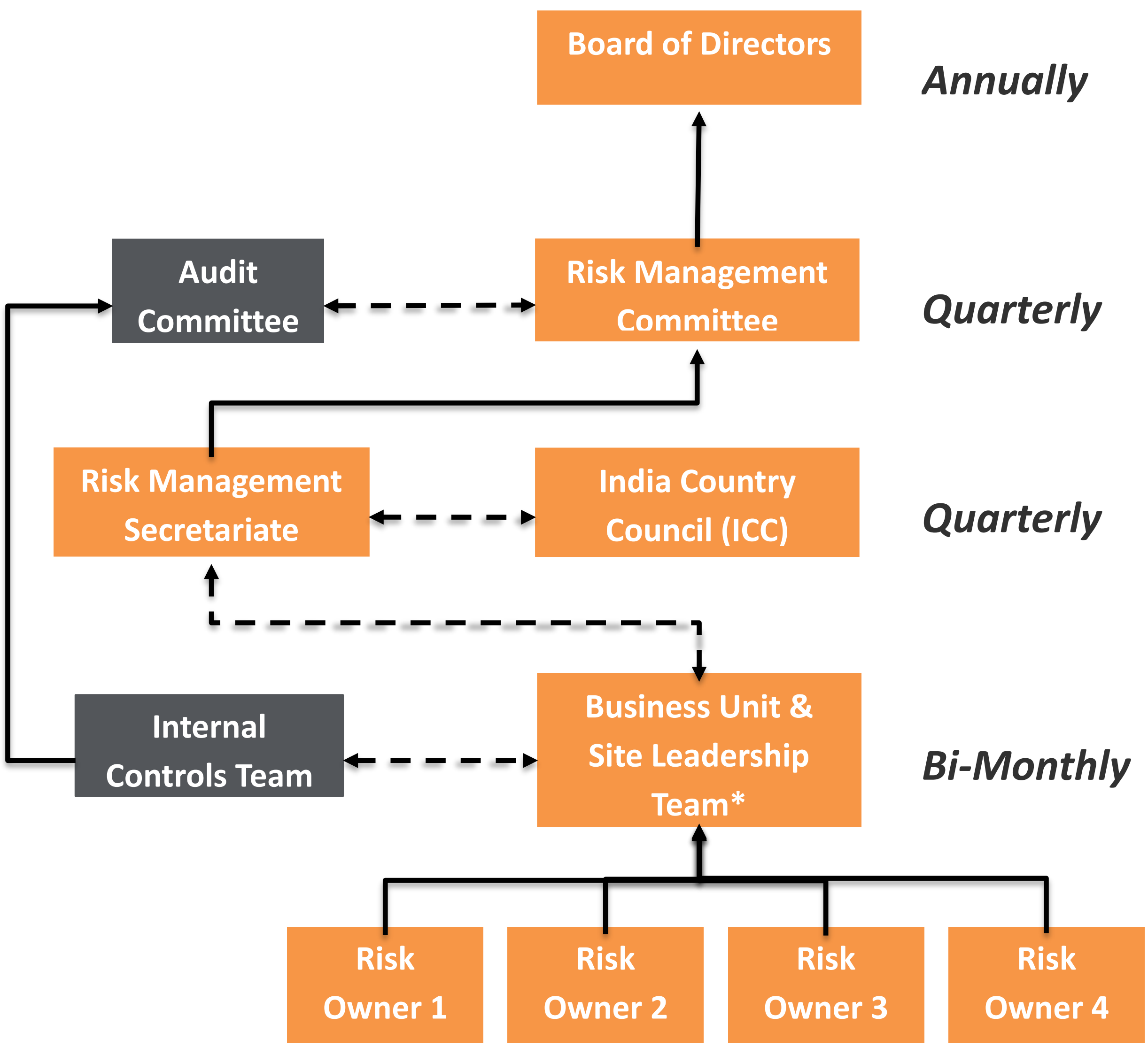
1. Consolidating all Risks faced by Sanofi so that the management / Board of Directors has full visibility on the risk events including business, financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the Risk Management Committee.
2. Enhancing capability to identify potential events that carry risks, establish responses for reducing surprises and associated costs or losses
3. Providing the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance
4. Enabling management to consider entity's risk appetite in evaluating strategic alternatives in business
5. Effectively assessing resource needs to prioritize and manage the potential risks

2. SCOPE

This policy applies to all commercial operations, manufacturing operations and sites located in all geographies across India. Under this policy, the Risk Management Committee may also rely on the Business Continuity Plan, which is a separate process, as may be necessary to mitigate any risk identified as part of this policy.

3. RISK GOVERNANCE FRAMEWORK

The following risk governance structure has been adopted by Sanofi to create a risk aware culture across the organization.



*Each business unit will have a BU risk coordinator who will be responsible to coordinate with the Risk Management Secretariate.

Risk Management Committee will be consisting of such members as may be decided by the Board of Directors. The Committee will nominate a senior employee to be Risk Coordinator of the Company.

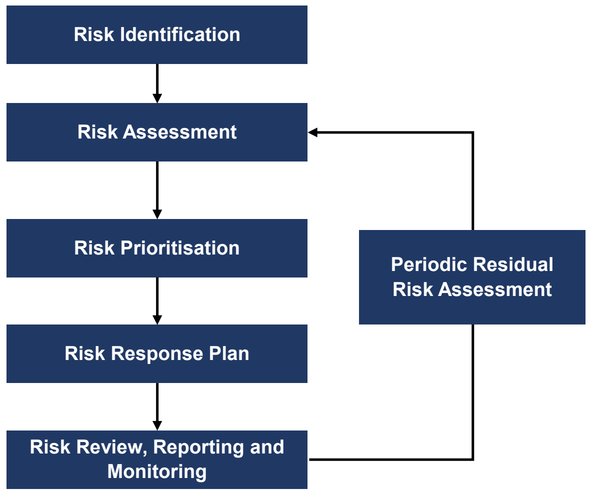
3.1 Roles and Responsibilities

Board of Directors	• The Board is fully committed to the objectives of ERM and its engagement in risk oversight function to strengthen the organizational resilience to significant risk exposures. ***The Board, through the Risk Management Committee shall oversee the establishment and implementation of an adequate system of risk management across the Company.*** • The Board shall comprehensively review the effectiveness of the Company's risk management system on **an annual basis.**
Audit Committee	• **Provide inputs to RMC on any other additional key risks and risk management framework**
Risk Management Committee	• The Board of Directors has constituted a sub-committee - Risk Management Committee (RMC or the Committee) to assist the Board in framing policy, guiding implementation, monitoring and reviewing the effectiveness of risk management policy and framework. The Committee will act as a forum to discuss and manage key risks. The RMC will meet **at least twice in a year** or more frequently as may be deemed necessary after evaluation of the risk matrix, crisis scenario, etc. The roles and responsibilities of the RMC have been defined as per the Board approved Charter • **Advise the Board of Directors and Audit Committee** on effectiveness of the risk management systems. • Keep the **board of directors informed** about the nature and content of RMC discussions and recommendations, as well as the actions to be taken. • Ensure that appropriate methodology, processes, and systems are in place to **monitor and evaluate** risks associated with business of the company. • **Monitor and oversee implementation** of the risk management policy, including evaluation of the adequacy of risk management systems. • Periodically **review** the policy, at least once in **two** years, considering the changing industry dynamics and evolving complexity. • **Review and approve the ERM framework** of the Company on a periodic basis. The Committee shall review and approve the risk management culture, processes and practices of the Company. • Review and approve the **Crisis Management Framework** of the Company and Crisis Response Plans for key crisis risk scenarios. • Establish and communicate **risk vision** and **philosophy**, approve **risk strategy** and establish **risk appetite.** • Review and analyze risk exposure related to **key risks** and ensure that risk assessment and implementation are carried out as per the defined policies, procedures and plans.

	• Monitor and review the **exposures of the key risks** and assess management preparedness to deal with the risk and associated events. • **Engage other stakeholders** in the risk management process when the need is identified. Facilitate communication of ERM information. • The Committee may form and delegate authority to a sub-committee, which shall assist the Committee to manage the ERM.
India Country Council	• **Review the key risks and provide inputs** • **Review the status of mitigation plans for the key risks and discuss the same with the risk owners**
Risk Management Secretariat	Risk Management Secretariat shall be responsible for overseeing the implementation of the risk management policy. A designated Risk Manager will co-ordinate the activities of the Risk Management Secretariat. Risk Management Secretariat will be responsible for following: • Understand, accept and implement Risk Management processes. • **Tracking and monitoring** implementation including the timelines. • **Receive reports from Risk Champions and Risk Owners,** review risk management activities and compile the risk register.
BU Unit & Site Leadership Team	Roles and responsibilities of BU leadership team are as follows • **Review and update** the risk registers on a **Bi-Monthly** basis for their respective BUs. • **Identifies new plausible risks** which can have impact on their specific BUs. • **Nominate a BU risk coordinator** who will coordinate with the Risk Management Secretariate on risk matters.
Risk Owner (Normally a business head or functional head)	• Responsible for **identifying risks** and developing the respective **response plans** within his/her function(s) • **Perform** ongoing **assessment** of the risk(s) • **Periodic review, monitoring** and updating the progress of the risk(s)

RISK MANAGEMENT PROCESS

Risk management is a continuous process to identify, assess, and respond to risks facing the organization, according to the following steps.



3.1 Risk Identification

Business / Functional Heads are responsible for identifying risks, as well as associated threats and opportunities, in their respective perimeters, and acting as / appointing owners for these risks. The risks must be described and their root causes and consequences identified and analyzed.

Inherent Risk is typically defined as the level of risk in place in order to achieve an entity's objectives and before actions are taken to alter the risk's impact or likelihood.

Residual Risk is the remaining level of risk following the development and implementation of the entity's response

Risk identification is an ongoing process. Each business/enabling function of an entity will collate their risks in a risk register (Refer Exhibit 1) Entity level risk registers will be developed by combining the business/enabling function risk register Each identified risk will be assigned to a risk owner

In case of risks shared between several business / functions, the ownership must be agreed with departments impacted and reported as necessary to the Risk Management Committee to ensure optimal coordination and prevent duplication of efforts.

Sanofi has implemented a risk identification process to identify potential future events that could affect a category/categories of assets critical to the execution of business model of entities, business functions, enabling functions and/or group.

Sanofi has identified following Risk Categories:

Risk categories	Definition
Financial (F)	Inappropriate management of funds, frauds leading to losses, inappropriate payment to vendors, sellers, partners and/or customers.
Operational (O)	Risks that may disrupt defined business process/operations, inefficient use of resources etc.
Reputational (R)	Risk of a potential tarnished reputation, loss of marketplace or investor confidence caused by legal/regulatory breach, other reputational-impacting event
Regulatory (R)	Potential fines, litigation costs or enforcement actions from regulators resulting from changes in the legal and regulatory environment, perceived or actual conflicts of interest, and potential actions or breaches of compliance.
Extended enterprise (E)	Risk of potential disruption caused by a failure to identify, measure and mitigate risks at key third-party organizations
Strategic (S)	Potential risk(s) that could disrupt the assumptions at the core of an organization's business strategy
Sustainability (S)	Risks arising due to environmental, social or governance events
Technological (T)	Risk arising from operating technology and Information Technology etc.

4.2 Risk Assessment

Risks identified in the previous step will be assessed on the basis of the Risk Rating criteria.

Risk Rating: This framework sets up the risk rating criteria at Sanofi. Risk rating criteria is used for evaluation and prioritisation of identified risks.

Risk assessment involves analysing and evaluating the probable impact and likelihood of risk occurrence.

Impact of a risk on the stated objectives and goals: The degree of consequences to the organization should the event occur. Sanofi has developed impact scales for rating the impact for each parameter as defined below:

4.2.1 I**mpact parameter**s

Grading	Very Low	Low	Medium	High	Very High
	1	**2**	**3**	**4**	**5**
Financial – Revenue	Revenue Impact of less than < 2%	Revenue Impact of more than 2% and less than 5%	Revenue Impact of more than 5 % and less than 7 %	Revenue Impact of more than 7 % and less than 9%	Revenue Impact of more than 9%
Financial-PBT	PBT Impact of less than 2%	PBT Impact of more than 2% and less than 9%	PBT Impact of more than 9% and less than 14%	PBT Impact of more than 14% less than-18%	PBT Impact of more than 18%
Regulatory / Compliance	➢ Violation of Company policies and rules	➢ Minor non-compliances to laws resulting in nominal fines/ notices or order for improvement ➢ Order for business improvement ➢ Nominal fines **(< than Rs. 50,000)** ➢ Non-compliance with state level laws	➢ Administrative/ judicial punishment or order for business improvement at state level ➢ Litigation at state or tribunal level ➢ Fines **(Rs 50,000 to Rs. 4,00,000)** ➢ Order for business improvement ➢ Non-compliance with state level laws	➢ Non-Compliance to laws and regulations at an national/global level ➢ Judicial punishment or order for business improvement from a Government Body. ➢ High Fines **(Rs. 4,00,000 to Rs. 7,00,000)** ➢ Order for business improvement from a Govt. bodies ➢ Business suspension - revocation of permits/ license, suspension of production and sales	➢ Heavy judicial punishment at a national/ global level ➢ Temporary suspension order for a facility ➢ High Fines **(Rs. 7,00,000 to Rs. 10,00,000)** ➢ Non-compliance with national laws resulting in heavy penalties or prosecution ➢ Business suspension - revocation of permits/ license, suspension of production and sales

Grading	Very Low	Low	Medium	High	Very High
	1	2	3	4	5
Business Continuity	**Minor disruption** at the individual **business/ site level**	**Short term** disruption at the **individual business/ site level**	**Medium term disruption** at the **individual business/site level**	**Medium term disruption** at **organizational level**	**Sustained period** of disruption at the **organizational level**
Reputation/ Brand	➢ **Insignificant level damage** to company reputation and brand at **local/regional level** ➢ **Rumors** but no media coverage, no public concerns voiced	➢ **Low level damage** to company reputation and brand at **regional level** ➢ **Local media coverage** but no negative publicity, public concerns voiced ➢ **Scattered** spread on social media	➢ **High level damage** to company reputation and brand at **regional level** ➢ **Negative coverage** by major domestic media ➢ **Limited** social media spread	➢ **High level damage** to company reputation and brand at **national level** ➢ **Sustained negative coverage** by major domestic media ➢ **Viral spread** on social media for up to a **week**	➢ **High level damage** to company reputation and brand at **global level** ➢ **Sustained negative coverage** by major **global** media ➢ **Viral spread** on social media continuing effect for more than a **2-3 weeks**
Health Safety & Environment	➢ **Minor environmental** damage effects due to toxic / non-toxic factors ➢ **Damage without Health & Safety Concern**	➢ **Major environmental** damage effects due to toxic / non-toxic factors ➢ **Damage with Health & Safety Concern requiring first aid or small injury**	➢ **Serious environmental** damage effects due to toxic / non-toxic factors ➢ **Damage with Health & Safety Concern causing near miss cases**	➢ **Serious environmental** damage effects due to toxic / non-toxic factors and **prosecution** ➢ **Damage with Health & Safety Concern causing accident/ injury/ permanent disability**	➢ **Serious environmental** damage effects due to toxic / non-toxic factors **and prosecution & suspension of operations** ➢ **Damage with Health & Safety Concern causing fatality and loss of life**

- Note: *In case of multiple applicable impact criteria, the most stringent rating is chosen as the final impact score*

4.2.2. Likelihood Parameters

Likelihood	Description	Probability
Almost Certain (5)	Event expected to occur in most circumstances	80%- 99%
Likely (4)	Event will probably occur in certain circumstances.	60%- 80%
Possible (3)	Event should occur at some time	40%- 60%
Unlikely (2)	Event could occur at some time	20%- 40%
Rare (1)	Event may occur, but only under exceptional circumstances.	1%-20%

The final Risk Score of a risk will be :

"Risk Score = Risk Impact * Risk Likelihood"

4.3 Risk Prioritization

The risks are prioritized on the basis of **Risk Prioritization Score**.

Risk Prioritization Score = Risk Impact * Risk Likelihood

The maximum rating of all parameters will be considered as risk impact for risk prioritization score
The prioritization of risks allows the management to determine actions for risks mitigation, and to allocate the relevant budget and resources, in line with the level of risk exposure.

The management must prioritize risks taking into account their criticality based on the combination of their severity and likelihood as under:

Severity

Likelihood --> / Impact	1 (Rare)	2 (Unlikely)	3 (Possible)	4 (Likely)	5 (Almost Certain)
5 (Very High)	Low (5)	Medium (10)	Medium (15)	High(20)	High (25)
4 (High)	Low (4)	Low (8)	Medium (12)	Medium (16)	High (20)
3 (Medium)	Low (3)	Low (6)	Low (9)	Medium(12)	Medium (15)
2 (Low)	Low (2)	Low (4)	Low (6)	Low (8)	Medium (10)
1 (Very Low)	Low (1)	Low (2)	Low (3)	Low (4)	Low (5)

Risks will be prioritized basis the following criteria:

Risk Rating	Criteria
High	Risk Score >= 20
Medium	Risk score >= 10 and < 20
Low	Risk score < 10

4.3.1. Assess Residual Risk

Perform Residual Risk Assessment as per the defined methodology. Please refer the below methodology:

Risk Response Effectiveness Categorization	**Low effectiveness**	**Medium effectiveness**	**High effectiveness**
Level of response over risk	**Low**	**Medium**	**High**
Response measure description	Risk is largely outside the control of the Management	Risk Response Action Plans may only reduce Risk to a medium level	Risk Response Action Plans deemed to be able to reduce risk to Low level
Impact of response	As per management estimate, the existing mitigation measure will reduce the gross impact / likelihood by 10% or lesser	As per management estimate, the existing mitigation measure will reduce the gross impact / likelihood by 10% - 30%	As per management estimate, the existing mitigation measure will reduce the gross impact / likelihood by 30% - 70%
Residual Impact Assessment Score	Gross Risk Score for Impact*0.9 And rounded off to nearest integer or 1, whichever is higher	Gross Risk Score for Impact*0.7 And rounded off to nearest integer or 1, whichever is higher	Gross Risk Score for Impact*0.3 And rounded off to nearest integer or 1, whichever is higher
Residual Likelihood Assessment Score	Gross Risk Score for Likelihood*0.9 And rounded off to nearest integer or 1, whichever is higher	Gross Risk Score for Likelihood*0.7 And rounded off to nearest integer or 1, whichever is higher	Gross Risk Score for Likelihood*0.3 And rounded off to nearest integer or 1, whichever is higher

Example:

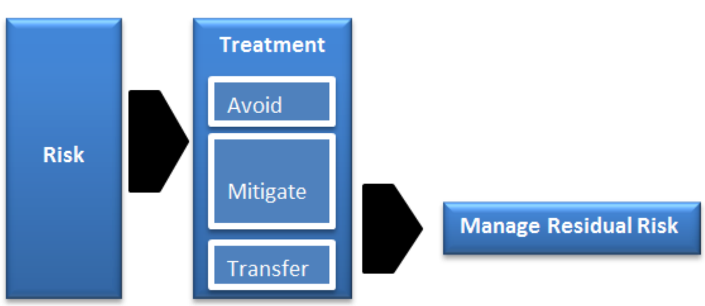
Example of Residual Risk Assessment													
Inherent Risk Score (Before implementation of Risk Response Plans)				Risk Response Effectiveness Rating						Residual Risk Score and Rating			
Impact	Likelihood	Score	Risk Rating	Low (10%) RRF* (0.9)		Medium (30%) RRF* (0.7)		High (70%) RRF* (0.3)		Impact	Likelihood	Score	Risk Rating
				I	L	I	L	I	L				
4	3	12	High	✓	✓					4*0.9=4	3*0.9= 3	12	High
3	4	12	High			✓	✓			3*0.7=2	4*0.7= 3	6	Medium
5	5	25	Critical					✓	✓	5*0.3=2	5*0.3= 2	4	Low

RRF Risk Response Factor (30%, 70% and 90% i.e. 0.3, 0.7 and 0.9) are assumed percentages and may change on case to case basis

4.4 Risk Response Plan Treat and reduce exposure

Risk Response Planning involves identifying the most appropriate strategies to manage risks and reduce them to an acceptable level .. Risk Response will include the following action steps:

The Sanofi risk treatment strategy depends on the risk tolerance. It must balance efforts and benefits for Sanofi maintaining its compliance to legal, regulatory and other requirements such as social responsibility.



Strategy	Description
Avoid	This strategy should be deployed when risks are unacceptable. In such cases, the activities linked to the risk should be stopped or comprehensive controls / changes in the activities underlying processes should be implemented to reduce risk exposure
Mitigate	Implementing methods / solutions that reduce the frequency or impact of risk. Relevant business / function must make sure that mitigation plan for each such instance is prepared and followed up.
Transfer	Risk is mitigated by having another party accepting the risk, partly or totally, typically through hedging, insurance, sub-contracting arrangements (attention to be put on residual risk resulting from sub-contractor)

To achieve its strategic objectives and create long term value, Sanofi is willing to take certain risks. It is the responsibility of the Managing Director to approve risk appetite and risk tolerance for each risk type in consultation with Risk Management Committee and Risk Coordinator.

4.5 Risk Review, Reporting and Monitoring

In order to ensure that risk management is effective Sanofi has set up a risk reporting, monitoring and review process. Risk reviews ensure evaluation of risks on a predetermined frequency at different levels to track the dynamics of the internal and external environment continuously. Risk review process at Sanofi will include the following action steps:

- Risk response plan owners will review the implementation status of risk response strategies and their defined action plans.
- Risk owners will update the ERM risk register template in consultation with risk response plan owners.
- Risk owners will re-assess risks as per the following frequency:

Risk Management Activity Calendar

S. No.	Activity	Responsibility	Frequency/Timelines
1.	Risk Identification	Risk Owners/Heads of Business Functions and Enabling Functions	Ongoing
2.	Prepare a risk response plan	Risk Owners	Ongoing
3.	Review status of implementation of Risk Response Plan	Risk Owners	Quarterly
4.	Review and assessment of risks	Risk Owners/Heads of Business Functions and Enabling Functions	Quarterly

S. No.	Activity	Responsibility	Frequency/Timelines
5.	Consolidation and Revision of individual Risk Registers into Enterprise Risk Register	Risk Management Secretariat	Quarterly
6	Update status of top risks	Risk Management Secretariat	Quarterly
7.	Presentation of top risks to Risk Management Committee (Risk Dashboard Presentation)	Risk Management Secretariat	Quarterly
8.	Reporting of top risks to the BoD	Risk Management Committee	Quarterly
9.	Provide inputs on Risk Management	Board	Annual

4. RISK CULTURE

Risk management Committee, Managing Director and Risk Management Secretariate will work towards creating a Risk identification and mitigation culture in the Company. This would include discussion on Risk in Management meetings and Risk communications.

5. REVIEW OF THE POLICY

Risk Management policy shall be reviewed at least once in a period of two years to check its effectiveness in the changing industry dynamics and evolving complexity.

Exhibit – 1

S.No	Risk Ref. No.	Function	Internal/ External	Risk Category	Risk Statement	Contributing Factors	Risk Owner	Impact						
								Business Continuity - I	*Financial – Revenue - II*	*Financial- PBT - III*	*Regulatory /Compliance - IV*	*Reputation/ Brand - V*	*Health Safety & Environment - VI*	Final Impact Score (Highest among all the impact scores)

Basic Risk Information

1. Risk Number: The qualitative number assigned to the risk for its tracking at time of reporting
2. Function: Function which highlights the risks, for cross functional risks all the involved functions are to be mentioned here
3. Internal / External: Risks are classified based on their nature whether internal or external or both
4. Risk Category: Risks are prominently identified in view of the various categories so as to prepare an exhaustive risk register and avoid any risk being left out of the view.
5. Risk Statement: Risk Statement is a short description of the risk. It could be populated after describing cause and impact of the risk. It should ideally not run more than one or two sentences. Thus, the right choice of words for its articulation becomes utmost important. It could be populated after describing event, cause, and effects of the risk.
6. Contributing Factors: The possible reasons that could lead to risk event form its causes. This can be mapped using root cause analysis tools which must be used to arrive at the root causes
7. Risk Owner: Risk ownership should lie with someone whose objective gets impacted the most (irrespective of the fact of executing the mitigation steps) and would be senior enough to drive and coordinate the mitigation responses. Even where risks are collectively managed, a single risk owner should be named who will take the lead responsibility for monitoring the risk and its associated controls

Risk Assessment Information

1. Impact: All possible impacts the event may have on the organizational goals and strategies. This must be detailed using the scales defined in the risk assessment section of this document
2. Risk Impact: Risk impact means the consequences in case of occurrence of the risk. Each risk is rated on a scale of 1 to 5 based on the risk impact matrix.

Likelihood	Risk Score	Risk Rating	Response Strategy	Existing Response Plan/Controls	Planned Future Response Plan	Risk Response Owner	Target Date for Implementation of Risk Response Plan	Status of Risk Response Plan	Risk Score (Previous Qtr)	Risk Score (Current Qtr)	Risk Trend	Risk Reported Date	Key Risk Indicator

Risk Assessment Information

1. Risk Likelihood: The likelihood of risk hitting the aforesaid business drivers are assessed and graded as per risk likelihood matrix. Risk likelihood is graded to assess the probability of a risk event occurring, while the existing controls are in place. Each risk is rated on a scale of 1 to 5 based on the risk likelihood matrix.
2. Risk Score: Likelihood * Impact = Risk score. The highest of all risk scores computed for different impact scales form the risk score for the risk.
3. Risk Rating: This will be an auto populated column. Users will be able to see the level of risk based as defined in the criteria for risk prioritisation.

Risk Response information

1. Response Strategy: The most appropriate strategy to manage the risks and bring them down to an acceptable level. It has 4 strategies. Treat, Transfer, Terminate & Tolerate
2. Existing Response Plan/Controls: All actions completed till date to treat the risk.
3. Planned Future Response Plan: List of actions in progress / in pipeline to treat the risk
4. Risk Response Owner: Mention the name of the Individual who would be responsible to execute the Planned Future Response Plan
5. Target Date for Implementation of Risk Response Plan: Enter the date (DD-MMM-YY), expected timeline by which risk response plan will be implemented.
6. Status of Risk Response Plan: This gives the current status of the response plan which would be Implemented, not implemented, work in progress, NA

Risk Review, Monitoring and Reporting

1. Risk Score (Previous Qtr): Capture the risk score from previous quarter's risk register
2. Risk Score (Current Qtr): This will be auto populated from the current quarter's risk score
3. Risk Trend: This will be an auto populated column which will compare current and previous quarter scores and generate a trend (upward, downward, no change)
4. Risk Reported Date: Enter the date the risk (DD-MMM-YYY) was first reported
5. Key Risk Indicators: "Key Risk Indicators" are rule based quantitative or qualitative triggers from multiple sources of information for early identification of potentially harmful scenarios.