BAYER CROPSCIENCE LIMITED

RISK MANAGEMENT POLICY

1. INTRODUCTION

The success any organisation achieves depends on its ability to understand the challenges of a changing world and respond to it effectively. Doing business involves taking risks – every business decision involves risks as the actual impact of such decision often cannot be ascertained with accuracy in advance. It is important that the decision business takes is evaluated from a risk perspective and in that perspective, risk management is an integral part of corporate management.

A risk management system supports the management in achieving its future objectives and safeguarding the organisation against significant risks, as well as in the execution of management´s managerial, legal and regulatory responsibilities.

Bayer group's Internal Audit & Risk Management function has defined its mission as "We safeguard our Company against critical risks and strengthen its path to growth, building on trusted professionals and leading technologies. It provides independent and objective assurance as well as advisory services on behalf of the Board of Management."; the same has been adopted by Risk Management function for Bayer CropScience Limited (BCSL).

BCSL has established a systematic approach towards effective Risk Management in order to achieve the following objectives:

- establishment of a pro-active risk management culture across the organisation with a focus on risk transparency and effective risk treatment.
- enhancement of the organizational focus on significant risks.
- supporting line management in taking informed and risk-based decisions.
- systematic monitoring of risks and risk management effectiveness.
- systematic risk identification and management across functions.
- help comply with relevant regulatory requirements

BCSL's risk management policy (the Policy) outlines the risk management framework that Bayer has adopted and is intended to provide guidance to all employees on the risk management framework and its contents. The Policy explains the following aspects:

- overview of risk management
- structure of risk management organisation
- procedure for risk identification and its assessment

This Policy applies to all employees of BCSL and every part of its businesses and functions. The Policy complements and does not replace other existing compliance programs, such as those relating to environmental, quality and regulatory compliance matters etc.

2. OVERVIEW OF RISK MANAGEMENT

"Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives" – COSO Enterprise Risk Management Framework by Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Thus, risk management is a structured, consistent and continuous process which is applied across the entire organisation in order to identify potential events that could pose a risk to the organisation, assess the event for the risk it poses and manage the said risks.

To enable a consistent understanding of this policy, a glossary of risk related terminology is provided below:

Terminology	Explanation
Risk	happening or non-happening of an event which will have an impact on the achievement of objectives.
Risk Universe	a multi-level structure of potentially relevant risk categories.
Consequence/Impact	outcome of an event if it happens; threats have unfavourable consequences whereas opportunities have favourable consequences.
Likelihood of occurrence	chance that a particular event will occur; this is expressed as a probability of a single instance within a defined time period.
Risk identification	structured process to identify events that have an adverse impact on the achievement of the business objectives.
Risk assessment	process of estimating the likelihood of the event happening along with consequences of these identified events and comparing them against a defined risk acceptance threshold.
Risk analysis	overall process of risk identification and risk assessment.
Mitigation plan	measures that are currently in place and are directed towards reducing severity of consequences; either by way of reducing the probability of the event occurring or reducing the impact. *These measures could be of various types; point of time based (preventive, detective or corrective) or operative based (manual or automated).*
Gross level	level of risk that an organisation would face without taking account of any mitigation activities (i.e. controls) that are already in place
Net level	level of risk that an organisation would face after taking account of all mitigation activities (i.e. controls) that are in place; this depicts the current state of affairs of the Company.
Risk tolerance	it is measured as an acceptable/unacceptable range of variation relative to the achievement of a specific objective.
Risk response	measures that would be deployed in near future with an aim to further reduce the severity of consequences; either by way of reducing the probability of the event occurring or reducing the impact.
Risk Owner/Responsible	person with the accountability or authority to manage a risk

3. STRUCTURE OF RISK MANAGEMENT ORGANISATION

A risk management framework can be successfully implemented through a holistic combination of risk management structure, policies and procedures. A formal structure of risk management organization with clearly defined roles and responsibilities for risk management activities is an essential prerequisite for an effective framework.

The overall responsibility and accountability for implementing and sustaining effective risk management processes rests with the Board of Directors. The Risk Management Committee, organisation's management and other employees support and assist the Board of Directors in fulfilment of this responsibility.

In the below paragraphs, the role of various components of the risk management organisation is defined:

Board of Directors
The Board of Directors

- approves Risk Management Policy its associated procedures and practices.
- reviews and approves Company's risk tolerance levels.
- reviews the overall risk management practices and its robustness.
- include in its report a statement on risk management framework.

Audit Committee
The Audit Committee

- reviews the Risk Management Policy, its associated procedures and practices.
- reviews and approve the risk tolerances of the Company.
- evaluates if risk management system is in place by reviewing the practices followed and assessing its overall robustness.

Risk Management Committee
The Risk Management Committee is a cross-functional oversight body that shall ensure a holistic and balanced oversight on risks and their respective treatment. The composition of the Risk Management Committee to be in line with the SEBI (Listing Obligations and Disclosure Requirements) requirements. The Risk Management Committee shall comprise of:

1. Minimum three members, with a majority of them being members of the Board of Directors
2. At least one of the three members to be an independent director

The Board of BCSL has the powers to change the constitution of the Risk Management Committee as may be appropriate and the said revised constitution shall be considered to be part of this Risk Management Policy.

Further, Lead Risk Management, India shall be a permanent invitee to the Risk Management Committee. The Committee may invite other department representatives on need basis. The Risk Management Committee shall ordinarily meet for such number of times as mandated by SEBI's (Listing Obligations and Disclosure Requirements) Regulations; any additional meeting may be convened to discuss urgent business matters.

The Risk Management Committee is responsible for:

- To formulate a detailed risk management policy which shall include:
    - A framework for identification of internal and external risks specifically faced by the listed entity, in particular including financial, operational, sectoral, sustainability (particularly, Environment, Social & Governance (ESG) related risks), information, cyber security, legal and regulatory risks or any other risk as may be determined by the Committee.
    - Measures for risk mitigation including systems and processes for internal control of identified risks.
    - Business Continuity Plan.
- To ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company.
- To monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems.
- To periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity.
- To keep the board of directors informed about the nature and content of its discussions, recommendations and actions to be taken.
- The appointment, removal and terms of remuneration of the Chief Risk Officer (if any) shall be subject to review by the Risk Management Committee.
- Supporting the executive management in the establishment of a culture which balances risks and opportunities facilitated by conscious risk-based decisions.

The abovementioned role/terms of the Risk Management Committee shall be read in conjunction with the SEBI (Listing Obligations & Disclosure Requirements), 2015 as amended from time to time. Any subsequent amendment to the role of the Risk Management Committee as per the SEBI

Listing Regulations shall apply mutatis mutandis to the terms of reference/role of Risk Management Committee as mentioned herein.

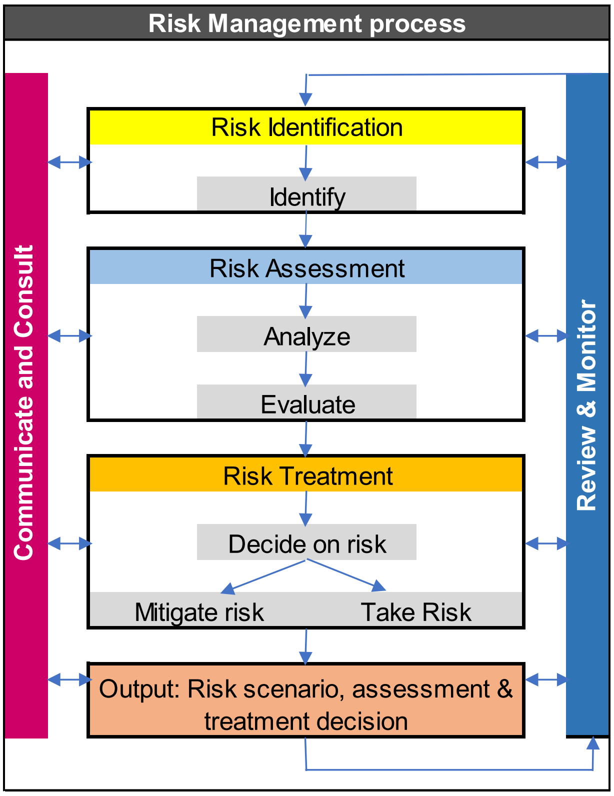
Risk owners
Risk Owners are a part of the local management organization. They are responsible for:
- implementing risk management activities within their sphere of responsibility,
- managing their risks by identifying, monitoring, treating and accepting them,
- reviewing as well as updating the risk portfolio and thereby ensuring completeness, adequateness of treatment strategy decisions and progress of risk mitigation actions.

Local Risk Management team
The local Risk Management department is the owner of overall risk management process within the organisation. The team is required to
- coordinate with various risk owners and other components of the Risk Management Structure for implementing the risk management framework in a comprehensive and holistic manner.
- ensure adequate documentation of the entire risk management exercise.
- review the risks as well as status of the mitigation plans and report to the Risk Management Committee.

4. APPROACH TO RISK MANAGEMENT

Risk management is a continuous activity and consists of various activities; beginning with risk identification and followed sequentially by risk assessment, controls assessment, risk review and monitoring and deciding on risk treatment. An overview of the risk management process is shown in diagram below followed by a more detailed explanation in the following paragraphs.

Figure 1 : risk management process



Risk Identification
The purpose of risk identification is to identify events which may impact the divisional/ functional short, mid or long-term objectives in a negative way.

The identification of risks is the first step in the risk management process. The aim of risk identification step is to collect and document all currently knowable risks which could affect achievement of the objectives. Risks can be identified using a number of different techniques, either through one-to-one interview with individual Risk Owner or in a workshop with a group of Risk Owners. The one-to-one interviews/workshop shall be followed by discussion with senior management wherein already identified risks can be confirmed/clarified as well as new risks could be identified.

Discussion with Risk Owners should begin by seeking an understanding of their department/ function level objective and scenarios in which an event could result in a risk to the achievement of these objectives. In order to assist in the process of identifying risks, a range of potential events need to be considered for discussion. To support a complete identification of potential risks, it is advisable to revisit all relevant sources of data; this could include recent internal or external incidents, existing risk information from audits, external industry sources, domestic as well as international trends etc.

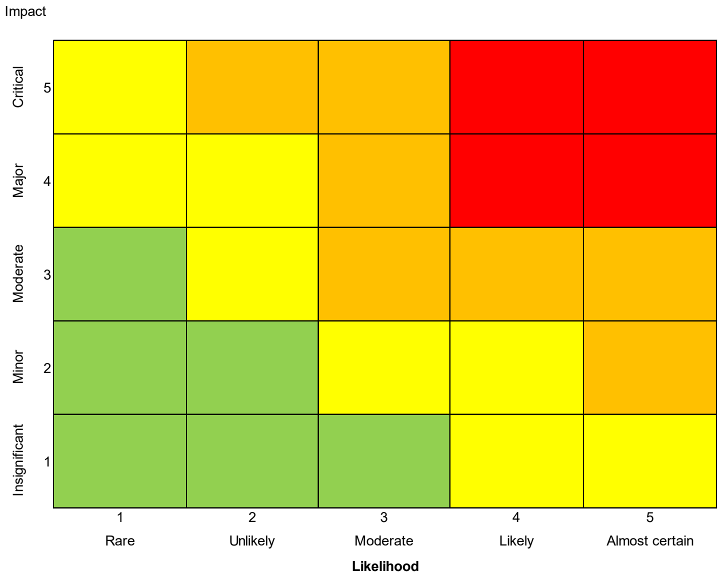
Risks that are identified need to be documented in a Risk Register, at a level of detail so as to support its subsequent assessment and management. Risk Register acts as a central repository and is meant to record risks and its related information in a structured manner. The risk description should explain 'cause' and 'effect' of the risk and thereby allow an independent person to gain a good understanding of the event posing a risk to the function. It is recommended not to perform risk assessment during the risk identification process in order to minimise bias.

Risk Assessment
Assessment of a risk involves quantification of impact of risk to determine its potential severity and probability of its occurrence.

Objective of risk assessment is to determine the risk level for each identified risk; such determination is done by using two parameters viz. Likelihood of Occurrence and Impact. Likelihood of Occurrence measures the probability of the event happening which shall result in a risk to the organisation. Impact measures the potential consequence of the event in terms of quantitative as well as qualitative parameters. A mix of various quantitative and qualitative criteria is considered for ascertaining the Impact and thereby make the assessment process a holistic exercise. For measuring the Likelihood of Occurrence and Impact, a 5-point scale is used. For Likelihood of Occurrence, it ranges from 'rare' (1) to 'almost certain' (5), and for Impact from 'insignificant' (1) to 'critical' (5).

To understand the strength of mitigation plans, it is necessary to assess the risks under two scenarios – first assuming that none of the existing mitigating controls would be in place and secondly considering all the existing mitigating controls would be in place as of date. Assessing risks assuming complete absence of any mitigating controls is called as Gross level of risk. This helps an organisation to ascertain the maximum impact that it shall face in case that particular risk materialises. However, in reality, every organisation does implement certain risk mitigation measures which are reflected in its existing state of affairs; this state depicts the Net level of risk. It is important to note that mitigating controls still in planning or implementation phase must not be considered while making risk assessment at Net level.

The risk rating score at each level (i.e. Gross as well as Net) is based on a multiple of score of Likelihood of Occurrence and Impact and the same is plotted on the Risk Heat Map.
Figure 2 : 5 x 5 Risk Heat Map



Such a formal risk assessment (across two parameters and two scenarios) allows an organisation to focus on key risks and prioritize allocation of resources for its resolution.

Risk review and monitoring

Risk review involves reporting of risks to the oversight bodies for their review and seeking their views, passing these to the risk owners and assisting them in conduct of regular monitoring; all this to ensure that risk management is an ongoing exercise.

The results of the risk identification and assessment process (based on 5x5 scale) must be documented and reported to key stakeholders. The Risk Management Committee, in its oversight role, will review the risks to satisfy themselves of the effectiveness of the overall risk management framework. Risk review shall involve the following:

- assessing completeness of the Risk Register and validity of risks recorded therein.
- understanding changes in business model, functional processes, operating and regulatory environment since the previous assessment cycle and the corresponding changes necessitated in the risk profile of the organisation.
- reviewing effectiveness and implementation of actions plans for identified risks and revision in action plans.

Such a review mechanism of key risk information is important to ensure that all significant risks identified are considered in the context of the overall operations in a coordinated and consistent manner. This helps to highlight the key risks to senior management so as to seek their response and inputs with regard to key risks; leaving the 'not so important' risks to other executives in the organisation.

Risk Treatment

After the assessment of each risk has been completed across both the scenarios (Gross level and Net level) using both the parameters (viz. Likelihood of Occurrence and Impact), the Risk Owners can decide on ways to further reduce the Net level of risk. This would depend on the tolerance that the Risk Owners have defined for their objective achievement and the impact that an event would pose to the objective achievement. If a particular event would adversely affect the achievement of objective beyond the acceptable tolerance limit, then the Risk Owner has to consider ways to implement additional mitigation plans either to reduce the impact to an acceptable level or to manage the likelihood of event occurring.

The typical manner of implementing further risk mitigation measures can be broadly categorised into:

- Risk Avoidance: withdrawal from activities in case where additional risk mitigation measures are not cost effective and returns are unattractive in relation to the risks faced.
- Risk Acceptance: accepting the risk as additional risk mitigation measures are not cost effective; but the potential returns are attractive in relation to the risks faced.
- Risk Reduction: initiating steps or measures in order to reduce probability of risk crystallizing and/or reduce severity of its impact should the risk crystallize.
- Risk Sharing: measures designed to transfer the risk to a third-party.

The decided plan of action needs to be captured in the Risk Register along with the time frame by which the Risk Owners intend to implement such steps. Such action plan would be monitored for its implementation by the Risk Owners along with the Local Risk Management Team as a part of the Risk review and monitoring phase.

5. AMENDMENTS TO POLICY:

Any change in the Policy shall be approved by the Board of Directors on the recommendation of the Risk Management Committee. Any subsequent amendment / modification in the SEBI LODR Regulations, Act and all other applicable laws in this regard shall automatically apply to this Policy and be binding on the Company and shall prevail over this Policy, even if not incorporated in the Policy. In any circumstance where the terms of the Policy differ from any applicable law for the time being in force, the provisions of such applicable law shall take precedence over the Policy.

6. DATE OF APPROVAL & AMENDMENT, IF ANY:

The Board of Directors of the Company have adopted this Policy effective from November 7, 2014. This Policy was amended by the Board of Directors of the Company effect from November 01, 2021, and thereafter on February 11, 2025.
