# RISK MANAGEMENT POLICY

**SAUDI BASIC INDUSTRIES CORPORATION (SABIC)**

| | |
|---|---|
| Policy Owner | Chief Executive Officer |
| Approved By | Board of Directors |
| Date | 31/07/2025 |
| Version | 3 |



CHEMISTRY THAT MATTERS™

## 1. Purpose

1.1. The purpose of the Saudi Basic Industries Corporation ('SABIC' or the 'Company') Risk Management Policy (the 'Policy') is to ensure that SABIC has a consistent approach to proactively identifying, assessing, managing and monitoring key and emerging risks as well as implementing practical, cost-effective and robust business continuity plans (BCP) to resume and recover critical operations during business disruptions and emergencies, while also leveraging opportunities within SABIC's risk appetite. SABIC recognizes that effective risk and business continuity management is essential to safeguard operations, protect its reputation and provide resilience against disruptions. It also plays a key role in enabling SABIC to achieve its strategic goals. This Policy aims to support SABIC's culture of proactive risk management, promote regulatory compliance and create value through the establishment of principles by which all risks shall be managed. It also sets out some of the key responsibilities in respect of risk and business continuity management and oversight.

## 2. Application

2.1. This Policy applies to SABIC's Board and Committee Members, Executive Management, and employees ('Relevant Individuals') at SABIC. The Relevant Individuals are responsible for familiarizing themselves with and complying with the content of this Policy and documents that support this Policy. Non-compliance with this Policy may result in disciplinary action in accordance with applicable laws and regulations.

## 3. Key Principles

The key principles in respect of this Policy are as follows:

3.1. Executive Management shall lead by example, allocating adequate resources, and demonstrating oversight, accountability and transparency in the implementation of risk management, business continuity management and risk transfer solutions.

3.2. Risk strategy including risk tolerance shall be set by the Board and considered by the business as part of operations and decision-making, with timely escalation of any concerns.

3.3. Risk and Business Continuity management frameworks shall be implemented to protect and create value through monitoring risks and resilience plans at appropriate management and Board levels while also ensuring compliance with relevant laws and regulations.

3.4. A culture of risk and business continuity awareness shall be embedded with a focus on continuous improvement and learning.

3.5. The institutionalization of risk management shall be embedded into key decision-making, strategic and operational processes to enable documenting, reporting and escalation, where necessary, through effective mechanisms.

3.6. Decisions shall be based on calculated risks that are guided by clearly defined risk matrix levels which are periodically reviewed and communicated.

3.7. Risks shall be identified, analyzed, evaluated within business units and corporate functions as part of the risk assessment process while ensuring internal controls and having robust risk response strategies (Avoid, Reduce, Transfer or Accept Risks) developed considering cost vs benefits, in consultation with the risk management team.

3.8. Current and emerging risks related to Strategic, Operational, Financial and Compliance (including cyber security, climate change, environment, and sustainability) shall be managed with appropriate arrangements in place to mitigate those risks and ensure acceptable levels of risks are not exceeded.

3.9. SABIC shall strive for continuous assessment and improvement of the risk and business continuity management systems in place.

3.10. The Risk and Business Continuity management teams shall operate as the second line of defense, ensuring that appropriate policies, procedures, and processes are in place, and overseeing the business appropriately.

3.11. Business impact analysis (BIA) shall be periodically conducted to identify all critical business processes and the scenarios that may disrupt them, along with implementing appropriate and cost-effective continuity strategies and solutions for all disruption scenarios, in consultation with the Business Continuity management team.

3.12. Business continuity plans (BCP) shall be developed and exercised/tested on an annual basis to ensure its relevance and effectiveness, in consultation with the Business Continuity management team.

3.13. Information on top, key and emerging risks (such as Key risk indicators, incidents and near misses, any other relevant risk data) shall be shared with Executive Management. Risks identified as having significant impact and occurring frequently shall be monitored carefully and be a key focus area.

3.14. Communication and consultation with appropriate external and internal stakeholders shall take place throughout all steps of the risk management process.

## 4. Policy Governance

4.1. This Policy shall be reviewed regularly by the Board, including when changes in business circumstances require it following recommendation from the Sustainability, Risk and EHSS Committee. The Policy Owner is the Chief Executive Officer (CEO) who, with support from the Executive Vice President Corporate Finance, is responsible for ensuring that it is communicated and implemented effectively and for monitoring ongoing compliance with the Policy.

## 5. Definitions

5.1.

| Terms | Explanation |
|---|---|
| Risk Management Framework | It is a set of components, which provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management practices throughout the organization |
| Risk Tolerance | is the boundaries of risk taking outside of which the organization is not prepared to venture in pursuit of its long term objectives |
| Risk Appetite | is the amount and type of risk that an organization is willing to pursue or retain |
| Business Continuity Management | Holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interest of its key stakeholders, reputation, brand and value-creating activities. |