

AKUMS DRUGS & PHARMACEUTICALS **LTD.**

RISK MANAGEMENT POLICY



AKUMS DRUGS & PHARMACEUTICALS LTD.

Regd. Office : 304, Mohan Place, L.S.C., Block – C, Saraswati Vihar, Delhi – 110034

**Corporate Office : Akums House, Plot no. 131 to 133, Block –C,
Mangolpuri Industrial Area, Phase – 1, Delhi – 110083**



1. Introduction

The Board of Directors of Akums Drugs and Pharmaceuticals Limited (“the Company”) has approved this Risk Management Policy in compliance with the provisions of the Companies Act, 2013 (“the Act”), which requires the Company to lay down procedures about risk assessment and risk minimization.

Risk management is an integral component of good corporate governance and fundamental in achieving the company’s strategic and operational objectives. It improves decision-making, defines opportunities and mitigates material events that may impact shareholder value.

2. Objective

Risk is an inherent aspect of a dynamic business environment. The Company is committed to high standards of business conduct and comprehensive risk management to:

- Protect the Company’s assets;
- Take risk adjusted business decisions;
- Ensure compliance with applicable legal and regulatory requirements; and
- Provide clear and strong basis for informed decision making at all levels of the Company.

This policy is intended to ensure that an effective risk management framework is established and implemented within the Company and to provide regular reports on the performance of that framework.



3. Definitions:

The Policy is formed around a common understanding of terminology used in this document i.e.:

- **Risk**

Risk is an adverse event resulting from inadequate or failed internal processes, people and systems, or from external sources. Risk can also be defined as any threat that can potentially prevent the Company from meeting its objectives. It also can be defined as a potential event or action that has a chance of occurring, which may result in a negative impact on the Company, its subsidiaries and its managed hospital.

- **Risk management**

It is defined as the systematic process of identifying, analysing, and responding to anticipated future events that have the potential to generate unwanted effects. It includes the ability to foresee challenges achieving the Company's objectives and attempts to lower the likelihood and impact of their occurrence.

- **Risk analysis**

It is the process of determining how often specified events may occur (likelihood) and the magnitude of their consequences (impact).

- **Risk evaluation**

It is the process used to determine Risk Management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria, to generate a prioritized list of risk for further monitoring and mitigation.

- **Risk assessment**

Risk Assessment is the combined process of Risk Analysis and Risk Evaluation.



- **Risk classification**

Risk elements are classified into various risk categories. Risks are grouped for better management and control. Each risk category is appropriately defined for the purpose of common understanding.

- **Risk review**

A risk review involves re-examination of all risks recorded in the risk register and risk profiles to ensure that the current assessments remain valid. It also aims at assessing the progress of risk treatment action plans.

- **Risk tolerance or risk appetite**

It indicates risk taking ability of the Company which will be qualitative in nature. It defines the risk scoring matrix to determine risk level and risk appetite codes indicating the Company's plan from zero tolerance to highest risk appetite level. Refer "Risk Appetite & Tolerance Guidance" for more details.

4. Roles and Responsibilities

(i) The Board:

- Approve and review the Risk Management Policy
- Define the Company's risk appetite
- Identify and assess internal and external risks in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk that may impact the Company in achieving its strategic objectives or may threaten the existence of the Company
- Define the role and responsibility of the Risk Management Committee and delegate monitoring and reviewing of the risk management plan to the Risk Management Committee and such other functions as it may deem fit, which also shall specifically covers the function related to the Cyber Security.
- Oversee the development and implementation of risk management framework and maintain an adequate monitoring and reporting mechanism.



(ii) Risk Management Committee

- 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, information, cyber security 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 committee to meet at as per the requirement of the Company.

(iii) Internal Audit:

Further, the independent Internal Audit function shall provide assurance on the integrity and robustness of the risk management process.



5. Risk management Process

i. Risk Universe Analysis:

Risk analysis involves consideration of the sources of risk, their consequences and the likelihood that those consequences may occur. The existing systems, control measures and procedures to control risk are identified and their effectiveness is assessed. The impact and likelihood of an event and its associated consequences are assessed in the context of the existing controls.

ii. Risk Identification

Risk Identification is obligatory on all vertical and functional heads that with the inputs from their team members are required to report the material risks to the Risk Management Committee along with their considered views and recommendations for risk mitigation. Analysis of all the risks thus identified shall be carried out by the Risk Management Committee through participation of the vertical/functional heads.

Risk Category	Description
Strategic Risks	<ul style="list-style-type: none"> • Market Strategy, Organizational Growth - Market Penetration, Market share, loss of reputation • Globalization and Technological obsolescence • Volatility in Commodity Market • Loss of Intellectual Property and Trade secret • Uncertainty surrounding political leadership in Domestic and International markets • Economic condition of the market, Global recession and Environmental Issues
Operational Risks	<ul style="list-style-type: none"> • Consistent Revenue growth • Cost Optimization • Manpower retention • Disaster Management and Data security • Inefficient working capital management - High Inventory
Compliance Risks	<ul style="list-style-type: none"> • Ensure stricter adherence to laws/ rules/ regulations/ standards • Adherence of company Policies and Procedures (SOPs)
Financial and Reporting risks	<ul style="list-style-type: none"> • Volatility in Currency, funding & Credit risk • Maintaining high standards of Corporate Governance and public disclosures



iii. Risk Assessment

Risk evaluation involves comparing the level of risk found during the analysis process against the pre-defined risk weights so as to assess their potential severity of loss and to the probability of occurrence. Risk weights of High / Medium / Low can be assigned based on parameters for each operating activity. The output of the risk evaluation is a prioritized list of risks for further action. If the resulting risks fall into the low or acceptable risk categories, they may be accepted with minimal further treatment.

Risk Assessment Matrix

Almost Certain	(5)	Low	Medium	High	High	High
Likely	(4)	Low	Low	Medium	High	High
Possible	(3)	Low	Low	Medium	Medium	High
Unlikely	(2)	Low	Low	Low	Low	Medium
Remote	(1)	Low	Low	Low	Low	Low
↑ Probability		(1)	(2)	(3)	(4)	(5)
→ Consequence		Insignificant	Minor	Moderate	Major	Catastrophic

Risk Score



iv. Risk Response

Risk response involves identifying the range of options for treating risk, assessing those options, preparing risk treatment plans and implementing them. Options include avoiding the risk, reducing the likelihood of the occurrence, reducing the consequences, transferring the risk, and retaining the risk. Gaps will then be identified between what mitigating steps are in place and what is desired. The action plans adopted will be documented and its implementation tracked as part of the reporting process. Ownership and responsibility for each of those risk mitigation steps will then be assigned. This will be captured in a 'Risk Assessment and Control Matrix' which comprising of the key top risks.



v. Reporting

The Executive Management should provide assurance to the Audit Committee and Risk Management Committee with regards to the financial records, risk management and internal compliance. Risks will be continuously monitored and reviewed; and the effectiveness of the controls in place and of the risk action plans is assessed to ensure changing circumstances do not alter risk priorities.

6. Documentation:

The responsibility for documenting the individual risks has been assigned to the risk owners. Hospital units and functionaries are responsible for performing and documenting risk assessments and developing appropriate risk management plan.

The key documents pertaining to risk management process that need to be maintained are:

- a) **Risk Register/ Risk library:** It contains a list of all identified risks during the periodic review. It is the key document used to communicate the current status of all known risks and is used for management control, reporting and reviews.
- b) **Risk Reporting Template:** The identified risks to be forwarded to the Risk Management Committee by the Executive Management for assessment.
- c) **Risk Profile/Risk Mitigation Plan Report:** The Risk Profile or Risk Mitigation Plan Report provides detailed documentation and attributes of risk along with details of actions planned for risk mitigation.



7. Policy Review

This policy shall be reviewed periodically, at least once in two years, including by considering the changing industry dynamics and evolving complexity to ensure effectiveness and that its continued application and relevance to the business. Feedback on the implementation and the effectiveness of the policy will be obtained from the risk reporting process, internal audits, and other available information