Enterprise Risk Management Policy and Guidelines

ศิครินทร์
SIKARIN

Sikarin Public Company Limited

Enterprise Risk Management Policy and Guidelines

Sikarin Public Company Limited (Sikarin) recognizes that risk is a critical factor influencing the long-term success and sustainability of the organization. A structured and comprehensive risk management approach is therefore essential to enhancing competitiveness and achieving Sikarin's vision, mission, and strategic objectives across economic, social, and environmental dimensions.

This Enterprise Risk Management (ERM) Policy and Guidelines have been established in alignment with the COSO Enterprise Risk Management Framework (2017 Edition) and incorporate applicable national and international standards. The aim is to elevate risk management practices and embed risk awareness into Sikarin's culture and decision-making processes at all levels.

Scope of the Policy

This Policy and Guidelines applies to Sikarin Public Company Limited, including all companies within the Sikarin Group (collectively referred to as the "Company" herein). It covers all aspects of risk management relevant to Sikarin's operations, ensuring a holistic, integrated, and continuous approach to managing risks.

Objectives

Sikarin Public Company Limited (the "Company") has established this Enterprise Risk Management Policy and Guidelines with the objective of creating a risk management system that is effective, transparent, and verifiable. This system is intended to support Sikarin's strategic direction across all dimensions—ranging from planning and policy formulation to operational implementation—in a systematic and integrated manner. The policy and guidelines also aims to enhance Sikarin's capacity for stable and sustainable growth, while creating shared value between Sikarin and its stakeholders, both internal and external. Furthermore, it seeks to build stakeholder confidence—particularly among the Board of Directors, senior executives, and other relevant parties—by reinforcing Sikarin's ability to effectively and promptly respond to uncertainty, business disruptions, and risk factors that may impact the achievement of its strategic objectives.

Roles and Responsibilities

Board of Directors

- Define Sikarin’s risk management policy and guidelines, direction, and framework in alignment with corporate strategy
- Approve the organization’s risk appetite
- Review the adequacy of the risk management system and processes at least annually
- Oversee and monitor risk management performance of the Enterprise Risk Management Committee and management team
- Provide policy-level guidance and promote a sustained risk-aware organizational culture

Risk Management Committee

- Establish strategies and plans that comprehensively address all categories of risk
- Assess systemic risks, enterprise-level risks, emerging risks, and ESG-related risks
- Continuously monitor, evaluate, and enhance the risk management system in response to changing business contexts
- Promote risk integration within all operational processes across departments
- Submit periodic risk management performance reports to the Board of Directors

Senior Management

- Implement risk management policies and plans relevant to their areas of responsibility
- Promote risk-informed planning and decision-making
- Regularly monitor and assess risk situations, and propose mitigation or improvement actions
- Support the development of risk management capabilities within their teams
- Report departmental risk performance to the Enterprise Risk Management Committee in a timely manner

Operational Units/Risk Owners

- Identify and assess risks related to their specific operational areas
- Develop appropriate risk treatment measures in line with identified risk levels

- Monitor and update risk control measures to ensure ongoing effectiveness
- Prepare and submit quarterly risk reports, or ad hoc reports in the event of significant incidents
- Coordinate with senior management to improve processes or internal control systems as needed

Internal Audit

- Evaluate the suitability and effectiveness of the risk management system through systematic audits
- Review compliance with risk-related policies, standards, and regulations
- Provide recommendations for enhancing risk management systems to ensure long-term resilience
- Report audit findings to the Audit Committee and the Board of Directors

Employees

- Perform duties in accordance with this policy and department-specific risk management protocols
- Stay aware of potential risks arising from their work, and participate in the identification, analysis, and timely reporting of risks
- Adhere to established risk controls, including safety, legal, and ethical standards
- Report any observed risks or anomalies through designated channels, such as direct reporting to supervisors or via Sikarin's incident reporting system
- Participate in training and learning activities to enhance risk management skills, understanding, and capability in their respective roles
- Contribute to building a corporate culture that values transparency, learning from failure, and shared responsibility in mitigating and managing risks at all levels

Guidelines

Sikarin Public Company Limited (the "Company") has established a comprehensive and contextually integrated risk management framework based on internationally recognized standards, including the COSO ERM Framework 2017, ISO 31000, and ESG and climate-related disclosure guidelines under IFRS S1 and S2. Sikarin's risk management framework is structured around five key components

Risk Identification

Risk identification is a critical first step aimed at understanding events that may affect the achievement of organizational objectives—at both strategic and operational levels. Sikarin adopts the following approach:

- Consider risks from both internal factors (e.g. organizational structure, operations, resources, personnel, and technology systems) and external factors (e.g. economic conditions, geopolitics, climate change, regulatory developments, and consumer behavior).
- Link risk identification with organizational context analysis, and incorporate ESG and climate-related risks, particularly at the strategic level.
- Refer to historical incident data, past failures, external reports, and industry databases to consistently identify emerging risks.
- Utilize a variety of techniques such as SWOT, PESTEL, Scenario Planning, Brainstorming, and RCSA (Risk & Control Self-Assessment) in collaboration with relevant units.

Risk Assessment and Prioritization

Sikarin applies both qualitative and quantitative assessment methods to determine which risks require priority management based on their severity:

- Assess risks by evaluating likelihood of occurrence and potential impact, using a Risk Matrix.
- Evaluate impacts across multiple dimensions, including financial, reputation, patient/customer safety, legal compliance, and ESG considerations.
- Define appropriate levels for Risk Appetite and Risk Tolerance, tailored to the nature of each risk category.
- Conduct risk aggregation at the enterprise level and risk prioritization to allocate resources effectively.

Risk Response

Risk response involves defining appropriate measures to reduce or control the impact of identified risks. Sikarin may adopt one or more of the following strategies:

- Avoidance – eliminating high-risk activities or projects that are not essential.

- Mitigation – developing internal controls or procedures to reduce the probability or impact of the risk.
- Transfer – shifting the risk to third parties, such as through insurance or contractual arrangements.
- Acceptance – accepting manageable levels of risk in line with cost-effectiveness and resource availability.

Risk response strategies must be supported by cost-benefit analysis and accompanied by a clear monitoring plan.

Monitoring and Reporting

Sikarin maintains a systematic process for monitoring, reviewing, and reporting risks to ensure that risk management remains effective:

- Continuously monitor risk status and control measures using Key Risk Indicators (KRIs).
- Report risk management performance to the Enterprise Risk Management Committee and the Board of Directors at least twice annually or in the event of a significant risk incident.
- Utilize internal audit as a key mechanism to evaluate the adequacy and effectiveness of the risk management process.
- Disclose ESG and climate-related risks in accordance with reporting frameworks such as IFRS S1/S2, TCFD, GRI, and Stock Exchange of Thailand requirements.

Enterprise-wide Risk Integration

Sikarin recognizes that effective risk management must be embedded into core systems and decision-making processes. The integration approach includes:

- Embedding risk management into strategic planning and capital allocation processes.
- Ensuring risk is a key consideration in decisions involving investments, new projects, business expansion, or policy changes.
- Aligning risk management with the internal control system and performance management frameworks.
- Promoting a risk-aware culture through training, communication, and defining risk ownership across all levels.

- Leveraging digital technology for real-time risk assessment and monitoring, such as dashboards, risk registers, and automated alerts.

Training and Capacity Building

Sikarin Public Company Limited places strong emphasis on continuously enhancing the knowledge, understanding, and skills necessary for effective risk management across all levels of the organization. The objective is to promote risk management as an integral part of Sikarin's culture and day-to-day operations. To this end, Sikarin provides regular in-depth training and awareness-building programs on key risk areas, including strategic risks, operational risks, ESG and climate-related risks, as well as legal, financial, technological, and cybersecurity issues. The effectiveness of these training initiatives is evaluated through post-training assessments, self-evaluations, or performance monitoring in real work scenarios, to ensure that employees are able to apply their knowledge appropriately in their roles—particularly within the healthcare service context, where decision-making often takes place under risk and uncertainty.

Disclosure and Transparency

Sikarin Public Company Limited is committed to operating with transparency and accountability. Sikarin discloses information related to risk management to all stakeholder groups through appropriate and timely channels. This includes disclosures regarding Sikarin's risk management framework, risk appetite levels, evaluations of risk management performance, key risk issues, and emerging risk trends. These disclosures are communicated through the Annual Report, Sustainability Report, One Report, and Sikarin's official website.

Policy Review and Update

Sikarin Public Company Limited requires that the Enterprise Risk Management Policy and Guidelines be reviewed and updated at least once a year, or when there are significant changes in laws, the business environment, risk scenarios, or stakeholder expectations. The review process is carried out by the Risk Management Committee in collaboration with management and relevant departments, under the supervision of the Board of Directors. This ensures that the policy and guidelines remains current and aligned with evolving global business trends and good corporate governance practices, both at the national and international levels. In addition, Sikarin will take into account the results of risk assessments, internal audits, stakeholder feedback, and information from risk trend reports as input for policy enhancement—ensuring that the policy remains comprehensive, effective, and responsive to emerging challenges.

The Enterprise Risk Management Policy and Guidelines is effective from 16 January 2025 onwards by the resolution of the Board of Directors at the meeting No. 1/2025 on 15 January 2025.

....

(Mr. Seni Chittakasaem)

Chairman