Fosun Group Guidance on Enterprise Risk Management

(Trial Version)

1. General Provisions

1.1. This guidance, formulated with reference to the relevant COSO frameworks,aims to assist Fosun Group ("the Group"), its subsidiaries and joint ventures (hereinafter referred to collectively as "the companies") to implement enterprise risk management, normalize risk management system, define risk management roles and responsibilities, improve the maturity level of risk management, and promote healthy, stable and sustainable development of the whole group.

1.2. Risk is the possibility that an event will occur and adversely affect the Group and the companies' achievement of business objectives.

1.3. Enterprise Risk Management("ERM") is the process, effected by the Group and the companies' board of directors, management and all other personnel, applied in a strategy setting and across each company within the Group, designed to identify potential events that may affect the Group and the companies, and manage risk to be within the risk appetite, to provide reasonable assurance regarding the achievement of enterprise objectives through executing risk management measures, cultivating risk awareness and risk culture, building up risk management system in daily operations. In the risk management process, the Group and the companies should monitor, prevent or mitigate key risks according to own situation.

1.4. The overall objective of ERM is to:

(1) Serve for decision making in strategy setting, investment and financing activities, balance overall risks and rewards, achieve the Group's strategic targets;

(2) Allocate resources efficiently, produce synergy effects, improve the effectiveness and efficiency of investment and business operations, further realize the Group's tactical business targets;

(3) Ensure the timeliness, accuracy, authenticity and integrity of operational and financial information;

(4) Ensure that the Group's investment and business operations comply with relevant laws and regulations.

1.5. The basic principles of ERM include:

(1) Consistency. The target of ERM should be consistent with the strategic business target.

(2) Compatibility. The capital of the Group and the companies should be compatible with the risks they take and the risks taken should be compatible with the rewards.

(3) Full coverage. The ERM should be implemented in each and every business and operation processes, covering all areas, branches, subsidiaries, departments, posts and staff and all types of potential risk. Each type of risk should be recognized, assessed and managed effectively.

(4) Materiality. ERM should be implemented in a practical and pragmatic way, focusing on key risks, significant risk events and internal control of key processes.

(5) Total involvement. Risk culture and relevant mechanism of full participation should be established. Staff at all levels should participate in risk management daily process according to their specific job duties.

(6) Combination of both quantitative and qualitative analysis. Develop risk quantification techniques, promote and apply risk management best practices according to the business nature, scale and complexity. Integrate quantitative and qualitative methods in managing risks.

(7) Continuous improvement. Risk management policies, guidelines and procedures should be adjusted and continuously improved against the assessment results of the real impact of changes in internal and external business environment and competitive landscape.

1.6. The main elements of ERM include but not limited to:

(1) Risk management organization;

(2) Risk management strategy, risk appetite and risk limits;

(3) Risk management policies and procedures;

(4) Risk management information system;

(5) Internal control and internal audit functions.

1.7. This guidance is applicable to the Group and its subsidiaries. Joint ventures may implement the present guidance by reference.

2. Risk classification

2.1. The risks the Group and the companies face in business operations mainly include:

(1) Strategic risk, the risk that corporate strategy is not compatible with market environment or corporate capabilities due to changes in the business environment or ineffectiveness in the development and implementation of strategies.

(2) Market risk, the risk of unexpected loss in positions arising from adverse movement in market prices such as interest rates, equity prices, real estate prices and exchange rates.

(3) Credit risk, the risk of unexpected loss stemming from a borrower or counterparty's failure to perform on an obligation, or adverse change in the borrower or counterparty's credit standing.

(4) Liquidity risk, the risk of being unable to pay the due obligations or meet other short term financial demands due to the inability to get enough capital in time or at reasonable cost.

(5) Operational risk, the risk of loss incurred for inadequate or failed internal processes, people and systems, or from external events, including legal risk.

(6) Compliance risk, the potential for litigation obligations, regulatory penalties, financial or reputation losses due to failure to comply with laws or regulations.

(7) Country risk, the risk of investing or operating in a foreign country or region, arising from possible economic, political, societal changes or events in local business environment that may adversely affect operating profits or the value of invested assets in the country or region.

(8) Reputation risk, the risk of loss resulting from damages to corporate reputation consequent to own business operations or an external event;

(9) Insurance risk, the risk of possible loss to an insurance company caused by deviation of actual mortality, morbidity, loss ratio, lapse ratio, etc. from the assumptions used in pricing.

(10) ESG risk, the medium and long-term risk due to failure to adapt to environmental and climate change, adverse changes in social and corporate governance, or missing

relevant development opportunities.

2.2. The Group and the companies should subdivide major types of risk into subclasses, review and update the risk classification according to own development stage, changes in business model, policies and procedures so to adapt to risk management requirements.

3. Risk Management Organization

3.1. The Group and the companies should set up risk governance structures; define clear roles and responsibilities in risk management for the board of directors, the management, functional departments, risk management department and internal audit department, covering all business units.

3.2. The board of directors of the Group ("the Board") is the highest decision-making body in ERM and takes the ultimate responsibility for the completeness and effectiveness of the ERM system. The responsibilities of the Board include:

(1) Approve the overall risk management objectives, risk appetite, risk limits and risk management strategy;

(2) Approve risk management policies and procedures;

(3) Oversee the Group's overall risk profile;

(4) Oversee the effectiveness of risk management and control process of the management;

(5) Approve the Group's ERM reports and information disclosure of various significant risks;

(6) Cultivate risk awareness and risk culture;

(7) Other related duties.

3.3. The Board may delegate the Risk Management Committee to execute part of its risk management duties, and to oversee the effectiveness of the operation of ERM.

3.4. Based on authorization by the Board, the Group's management (the Global Partners) is responsible for executing specific responsibilities of enterprise risk management in their areas of responsibility, which include:

(1) Take charge of the Group's daily risk management activities to ensure the overall risk is acceptable;

(2) Formulate and organize the implementation of ERM policies and procedures according to the risk management objectives and risk appetite approved by the Board;

(3) Set up the ERM organization, structure and internal accountabilities;

(4) Carry out periodical assessment of overall risk profile;

(5) Set up emergency management mechanism within the Group; analyze and develop solutions to significant risk events;

(6) Organize the development and application of risk management information system;

(7) Promote risk awareness and risk culture;

(8) Report to the Board on a periodical basis on the overall risk level and risk management status;

(9) Other duties authorized by the Board.

3.5. The Group and the companies should appoint Chief Risk Officer ("CRO") or designate other senior executive to take charge of ERM, whose duties mainly include formulating risk management policies and rules, coordinating the risk management work of various business

units and functional departments. The CRO should maintain sufficient independence and cannot be responsible for business activities such as investment and finance management. The CRO has the rights to know about major corporate decisions, significant risks, events, key systems and business processes, and participates in risk assessment and approval during the decision-making process.

3.6. The Group and the companies should designate or set up independent risk management function (line or department), equipped with enough qualified risk management professionals. The responsibilities of the risk management function include:

(1) Set up and maintain risk management system including risk management policies and procedures, corresponding roles and responsibilities and risk appetite, etc.;

(2) Assist and guide functional departments and business units to formulate risk control measures and solutions; propose criteria to determine major decisions, significant risks, events, and key business processes, and bring forward solutions for mitigating the risks;

(3) Identify risks and conduct qualitative and quantitative assessment in a periodical way; issue ERM reports and put forward management suggestions;

(4) Build and maintain risk management techniques and models; improve risk management methods constantly;

(5) Participate in asset liability management and propose suggestions to deal with risks, including the formulation of relevant policies and rules, selection of appropriate techniques, and effectively balancing risks and rewards of both assets and liabilities;

(6) Collect and sort risk related information of all departments; promote the establishment of the ERM information system;

(7) Other related duties.

3.7. All functional departments and business units should set up risk management procedures, assess and monitor own risks respectively. The risk management department ("the RMD") is responsible for organizing, coordinating and supervising the risk management activities of those departments and business units.

3.8. Through the setting-up of the above risk management organizations and structures, the risk oriented, four lines of defense model or four tiers of risk management framework is built up:

(1) The 1st line of defense is the business units and departments, who are responsible for identifying, assessing, responding, monitoring and reporting risks;

(2) The 2nd line of defense is comprised of functional departments such as legal, compliance, finance, human resource, quality and safety, the risk management department who assists the business departments in risk management;

(3) The 3rd line of defense is the internal audit department, who is responsible for oversight activities of the risk management policies, procedures established by the Group and risk control activities, and regularly report to the audit committee;

(4) The 4th line of defense is the anti-corruption department, whose duties are to protect both tangible and intangible assets of the Group, avoid loopholes of non-compliance with laws and regulations, corporate policies and procedures, and prevent illegal and criminal activities and fraud.

The 1st line of defense of business units and departments is the fundamental and most crucial line of defense within the ERM, taking the first and foremost responsibilities in ERM.

4. Risk Management Strategy, Risk Appetite and Risk Limits

4.1. The Group and the companies should develop a clear risk management strategy, review and assess its effectiveness at least once a year. The risk management strategy should reflect the risk appetite, risk profile and changes in market and macroeconomic environment.

4.2. Risk appetite is the amount and type of risk that an organization is willing to take in order to meet its strategic objectives, which reflects the organization's basic attitude toward risks. The Group and the companies should compile risk appetite statements, focusing on both quantitative and qualitative indicators.

The setting of risk appetite should be linked to strategic goal, business plan, capital plan, performance appraisal and compensation mechanism. Risk appetite should be conveyed and carried out throughout the organization.

4.3. The risk appetite statement should include but not limited to:

(1) The basis to set strategic goal and business plan; the linkage between risk appetite and strategic planning;

(2) The overall risk amount that the organization is willing to accept in pursuit of its strategic goal and business plan;

(3) The type of risk and the highest level of risk that the organization is willing to accept for various types of risk;

(4) Quantitative indicators of risk appetite, including profit, rate of return, risks, capital, liquidity, credit rating, etc., and their target values or range of values. The mechanism to integrate those indicators with business plan and performance appraisal, and the mechanism to cascade and set risk limits at increasing levels of granularity to business units, branches and subsidiaries.

(5) For risks that are inappropriate to quantify, qualitative descriptions are required including reasons of accepting the risks, their boundaries and measures taken to manage the risks;

(6) Capital adequacy and liquidity level required to defend the overall risk and specific types of risk;

(7) Circumstances that may lead to deviation of risk appetite targets, and the possible actions taken in case of occurrence.

The respective roles and responsibilities of the Board, management, the CRO, business lines, the RMD and the internal audit department should be clearly defined in the risk appetite statement.

Once risk appetite boundaries are breached, the Group and the companies should analyze the reasons, develop solutions and execute in time.

4.4. The Group and the companies should establish the mechanism to adjust risk appetite according to changes in strategic goals, business scale and complexities, and risk profile.

4.5. Risk limits are the result of further quantification of risk appetite and cascading risk appetite down to granular levels. Within the overall risk tolerance, risk limits are set for various operation standards that may impact the overall risk level and their risk indicators. These risk limits serve as the basis and standard for risk monitoring by business units, product and operation departments.

The Group and the companies should formulate risk limits management policies and

procedures, which cover the setting of risk limits, adjustment of limits, limit breach reporting and mitigating actions in case of a breach. On the basis of risk appetite, risk limits are set according to dimensions of asset type, industry/sector, region or currency, etc. Factors such as capital adequacy, risk concentration, liquidity, and trading purpose should be taken into account in developing risk limits.

The RMD should monitor and report risk limits to the Board and management.

5. Risk Management Policies and Procedures

5.1. The Group and the companies should set up comprehensive ERM system of policies and guidelines to define the risk management strategy, risk appetite, organization structure, performance appraisal method, risk management mechanism, and specify requirements for managing various types of risk such as strategic risk, market risk, credit risk, liquidity risk, operational risk, compliance risk, country risk, reputation risk and insurance risk.

5.2. Risk management policies and guidelines should be formulated to cover identification, assessment and measurement methods for various risks, quantitative and qualitative standards of risk indicators, and responsible persons. The roles and responsibilities of functional departments such as strategy management, investment management, finance, tax, actuarial, legal affairs, branding, risk management, internal audit, and anti-corruption departments should be defined for managing specific risks. The policies and guidelines should be reviewed and updated at least once a year, properly recorded and archived.

5.3. Risk management procedures are the whole process of a series of risk management activities which include risk identification and assessment, risk measurement, risk response and control, risk monitoring, early warning and risk reporting. Risk management procedures should help implement the established corporate strategy and be consistent with the risk culture.

(1) Risk Identification is the process of recognizing and understanding the risks in business operations. The characteristics, possible causes of the risks, driving factors and conditions of the risks can be identified in this process.

(2) Risk Assessment is the process of analyzing and evaluating the recognized risks. The possible impact of the risks on attainment of operation targets will be assessed and form the basis for risk management

(3) Risk Measurement is the process of measuring potential economic losses caused by the risks according to business nature, scale and complexity and visually reflecting the risk profile.

(4) Risk Response and Control. According to the risk assessment and measurement results, the Group and the companies should prepare risk response plans on corporate strategy and risk appetite. The risk response plan should include risk management objectives, relevant procedures, conditions and required resources, specific measures to take and management tools needed.

(5) Risk Monitoring is the process of monitoring changes and development trends of all quantifiable key risk indicators and unquantifiable risk factors, as well as the quality and effectiveness of risk management measures. The Group and the companies should set appropriate quantitative and qualitative monitoring standards, define risk indicators to monitor and reporting procedures according to characteristics of various risks.

(6) Risk Warning is the process of issuing risk alerts when risk indicators deviate from the standards and meet early warning criteria. The Group and the companies should establish an early warning system to ensure that significant risks can be identified and resolved in a timely basis within the complex external and internal environment.

(7) Risk Reporting is the process of compiling and issuing risk reports of different types and at different hierarchy of risk governance, which follows the established scopes, procedures and frequencies, to meet the diversified management needs. The Group and the companies should set up risk information transmission and reporting mechanism to facilitate managing risks both interactively and cross-functionally.

5.4. The Group and the companies should adopt suitable risk management tools to manage risks, which include but not limited to:

(1) Comprehensive budget management;

(2) Asset-liability management;

(3) Capital planning and allocation;

(4) Economic capital models;

(5) Sensitivity analysis, scenario analysis and stress testing;

(6) Emergency management and planning.

6. Risk Management Information System

6.1. The Group and the companies should set up risk management information system to meet own requirements on risk management.

6.2. The data in the risk management information system should meet the criteria of timeliness, accuracy, consistency and integrity

6.3. The effectiveness of the risk management information system should be assessed periodically. Updates should be made in accordance with changes in internal control and risk management processes.

7. Internal Control and Internal Audit

7.1. According to risk management strategies and objectives, the Group and the companies should reasonably determine risk control points of various business and management activities; take appropriate control measures; perform unified business processes and management processes to ensure proper and orderly operation.

7.2. The Group and the companies should include ERM into the scope of internal audit, annually review and evaluate the sufficiency and effectiveness of ERM. Internal audit report of ERM should be submitted directly to the board of directors and board of supervisors. The board of directors should urge the management to promptly take corrective measures on audit findings. The internal audit department should follow up and check the results of the remediation and report to the board of directors in time.

8. Oversight, Appraisal and Evaluation

8.1. The Group and the companies should set up accountability in risk management. The management is responsible for determining risk owners of major risks and assigning specific responsibilities to corresponding functional departments and business units. Any organization or individual violating relevant policies should be investigated and punished

accordingly.

8.2. The Group and the companies should develop methods for appraisal and evaluation of ERM. The robustness of risk management system and effectiveness of compliance with it should be incorporated into performance appraisal of functional departments, business units and managers to improve risk awareness and accountabilities of management at all levels.

8.3. Risk oversight includes supervision and inspections of the robustness, reasonableness and effectiveness of the ERM system. The Group and the companies should periodically analyze the design of the ERM framework and execution results. Any risk management deficiencies detected in the oversight process should be remediated promptly so as to improve the risk management system continuously.

9. Risk Culture

9.1. To ensure the attainment of risk management objectives, the Group and the companies should embed risk culture into the building of enterprise culture at all levels, through continuously improving risk management policies, guidelines and procedures, strengthening organizations and developing risk management information systems.

9.2. To promote the establishment of a systematic, standardized and efficient risk management system, risk awareness should be strengthened across the whole group and converted into common sense and conscious actions of all staff.

9.3. Risk awareness programs are advocated and promoted within the whole group, and should be included in new staff orientation and training during work.

10. Implementation

10.1. This guidance goes into effect after the approval of the Board.