UMEDIC GROUP BERHAD

[COMPANY NO.: 202101015347 (1415647-D)]
(Incorporated in Malaysia)

RISK MANAGEMENT HANDBOOK

1.0 WHAT IS ENTERPRISE RISK MANAGEMENT (ERM)?

ERM is an integrated and continuous process for managing enterprise-wide risks - including strategic, financial, operational, regulatory / compliance risks - in order to minimize unexpected performance variance and maximize intrinsic firm value. This process empowers the board and management to make more informed risk/return decisions by addressing fundamental requirements with respect to governance and policy (including risk appetite), risk analytics, risk management, and monitoring and reporting.

(***Risk or Opportunity) / Return = Impact (Consequence) x Likelihood*** (Probability)

1.1 ERM Fundamental Concept

Risk is a variable that can cause deviation from an expected outcome, and as such may affect the achievement of business objectives and the performance of the overall organization. 7 key fundamental concepts that influence a company's overall risk profile, namely Exposure, Volatility, Probability, Severity, Time Horizon, Correlation and Capital, as illustrated in the below Diagram 1:

Diagram 1, Source: COSO-ERM2017

1.2 ERM Key Attributes

There are 7 key attributes of evidenced-based continuous ERM: -

i. ERM is a continuous management process that provides early-warning indicators for business leaders.

ii. Strategic risk management receives the highest priority.

iii. Dynamic risk appetite drives risk policies to balance business objectives and prudent risk-taking.

iv. Risk optimization is the primary objective of ERM. Companies achieve this by influencing the shape of their risk/return bell curve.

v. ERM is embedded into business decisions at all three lines of defense, supported by integrated risk assessment and analytics.

vi. A collaborative dashboard reporting system delivers ongoing risk and performance monitoring.

vii. Performance feedback loops assure ERM effectiveness and support continuous improvement.

1.3 ERM Value To Stakeholders

i. Aligning risk appetite: ERM prioritizes the development of a risk appetite that aligns strategic objectives across the organization and among stakeholders. It then integrates risk appetite into daily business decisions.

ii. Prioritizing strategy: ERM prioritizes the organization's and stakeholder's strategic objectives by providing timely risk information necessary to their pursuit.

iii. Providing early warning indicators: ERM allows company leaders to identify potential risk events affecting stakeholders in time to respond.

iv. Enhancing transparency: Stakeholders, along with company leadership, can view risk information and integrate it into their decision-making.

v. Identifying opportunities: Opportunity is a corollary to risk. In managing risk, companies and their stakeholders can take greater advantage of unanticipated opportunities.

1.4 Key Objectives of Three Lines of Defense *(Diagram 2)*

Diagram 2, Source: COSO-ERM2017

i. First line of defense: Business units are focused on generating growth and profits (upside bias).

ii. Second line of defense: Risk and compliance units are focused on risk policies and limits, ongoing monitoring, and compliance with laws and regulations (downside bias).

iii. Third line of defense: The board of directors is focused on independent risk oversight (governance); the internal audit is focused on the adequacy of internal controls and the integrity of financial statements (assurance).

1.5 Types of Risks

i. Strategic/Business risk is the potential business and economic impact arising from an adverse business decision, corporate and business strategies,

ineffective implementation of such strategies, failure to respond to industry and technological changes, and insufficient business diversification.

ii. Financial risk is the potential business and economic impact resulting from adverse movements in market prices and rates, the borrower or counterparty defaults, and the inability to meet cash flow requirements in a timely and cost-effective manner.

iii. Operational risk is the potential business and economic impact resulting from human error or malfeasance, failed internal processes or systems, or external events and disasters.

iv. Regulatory/Compliance risk is the potential business and economic impacts, such as regulatory sanctions, financial loss, or damage to reputation, resulting from failure to comply with applicable laws and regulations.

2.0 PRINCIPLES AND STRUCTURE

2.1 Principles

The principles listed below are intended to provide a general policy framework for evaluating and reducing risks, while recognizing risk analysis is an evolving process.

i. The depth or extent of the analysis of the risks, benefits and costs associated with a decision should be commensurate with the nature and significance of the decision.

ii. Each risk owner should employ the best reasonably obtainable information from various sources to conduct risk assessment exercise.

iii. The categorization of risks and changes in the nature or magnitude of risks should be both qualitative & quantitative and consistent with available data.

iv. The risk categorization should be broad enough to inform the range of activities to reduce risks.

v. Judgment used in evaluating a risk assessment, such as assumptions, defaults, and uncertainties, should be stated explicitly. The rationale for these judgments and their influence on the risk assessments should be articulated.

vi. Peer / independent review of risk assessments should be maximized as it can ensure that the highest professional standards are maintained.

vii. In making risk management decisions with significant impact, Risk owner should analyze the distribution of the risks and the benefits and costs (both direct and indirect, both quantifiable and non-quantifiable) associated with the selection or implementation of risk management strategies.

viii. Risk owners should adhere to the Group's criteria and methods to evaluate the effectiveness of risk management decisions.

ix. Risk owners should adopt a risk mitigation strategy by avoiding, preventing, reducing, transferring and neutralizing risks and uncertainty.

x. Risk communication should involve the open, two-way exchange of information between professionals, including both policymakers and "experts" in relevant disciplines.

2.2 Reporting Structure

Notes:

-·-·-·-·-·-·-·- Functional Reporting

---------- Independent Feedback

3.0 ERM ROLES AND RESPONSIBILITIES

Board of Directors

- Establish board risk governance and oversight processes.

- Approve risk policies; link strategy and strategic risk management decisions.
- Accountable for periodic review and assurance of controls.

- Communicate the Group's risk profile to key stakeholders, including regulators, stock analysts, rating agencies, and business partners.

- Approve the risk management framework as well as the Group's risk appetite and tolerance.

- Review the adequacy and effectiveness of the Group's internal financial controls, operational and compliance controls established by the Management;

Audit and Risk Management Committee

- Oversee the overall development and effectiveness of the audit and risk management framework.

- Implementing board- and corporate-level reporting in all risk areas and regulatory compliance.

- Review specific risk assessments and focus areas, such as cybersecurity, anti-money laundering, bribery and corruption, third-party oversight and business contingency planning.

- Review and approve recommendations with respect to capital structure, dividend policy and target debt ratings, etc.

- Review and recommend strategic risk management decisions including major investments and transactions.

- Conduct periodic review of the registry of risk of the Group (at least once a year) and determine the acceptability of the residual risks of the Group.

Risk Management Working Group

- Establish the risk appetite and risk tolerance levels as well as other corporate risk policies.

- Provide overall leadership and vision for enterprise risk management including addressing change management requirements.

- Establish integrated risk management across separate business units in the organization.

- Oversee the risk-taking activities of the organization including organic and acquisition growth opportunities.

- Develop risk management policies and quantifying enterprise-wide risk appetite.

Risk Owners

- Ultimately accountable for business/risk management.

- Execute risk policies and standards, risk appetite and tolerances, and reporting processes.

- Establish and implement risk and compliance activities.

- Accountable for ongoing risk monitoring and oversight.

Outsourced Internal Audit

- Assess reporting of key risks and ensure that the risks are properly evaluated.

- Review the system of internal controls to determine their adequacy and effectiveness in relation to the key risks and to report the same to the Audit and Risk Management Committee.

- Review whether all relevant key risks have been identified and managed adequately for business activity under review and to report the same to the Audit and Risk Management Committee.

- Review whether all relevant key risks have been identified and managed adequately for business activity under review and to report the same to the Audit and Risk Management Committee.

- Verify compliance with the risk control measures embedded in the internal controls.

4.0 ERM FRAMEWORK

4.1 COSO-ERM 2017 Framework *(Diagram 3)*

The concept behind the COSO ERM 2017 framework is a set of four basic entity objectives. The framework breaks down these objectives in terms of control components and the organization's business structure. The first dimension of the framework provides four categories of entity objectives: -

i. Strategic: high level, mission-oriented goals

ii. Operations: effective and efficient resource usage

iii. Reporting: reliable information and communication

iv. Compliance: conformity to laws and regulations

The second dimension of the framework emphasizes on interconnected nature which includes: -

i. Internal Environment: shaping company culture, ethical values, risk perception and appetite.

ii. Objective Setting: creating goals within the four categories listed above.

iii. Event Identification: distinguishing between internal and external risks and opportunities.

iv. Risk Assessment: evaluating risk based on likelihood and impact.

v. Risk Response: deciding whether to avoid, accept, reduce, or share risk.

vi. Control Activities: establishing a procedural precedent to ensure an appropriate response.

vii. Information and Communication: capturing and sharing information to support informed decisions.

viii. Monitoring: continually evaluating and optimizing business and risk processes.

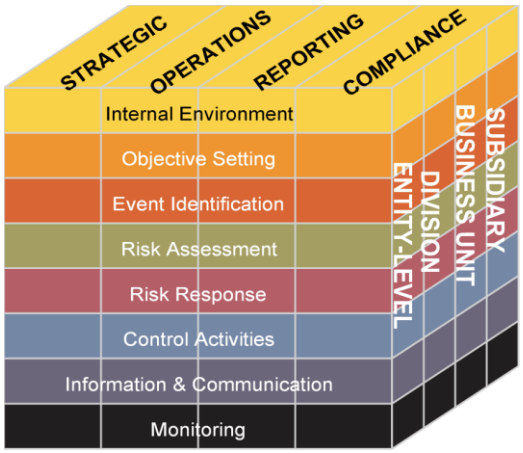

Diagram 3, Source: COSO-ERM2017

The third dimension to the framework in which all 4 objectives and 8 components above are broken down by the structural elements of the organization itself:

i. Entity-Level

ii. Division

iii. Business Unit

iv. Subsidiary

The idea behind the framework is to create a complete taxonomy of risk management, permitting evaluation and analysis at a granular level.

4.2 ERM Approach *(Diagram 4)*

Frequency	Events	Regulatory Requirements	Annual	Monthly/Quarterly	Continuous
Scope	Tactical Response	Regulatory Defined	Operational	Financial	Strategic
Risk Appetite	Disaster Avoidance	Regulation Based	Internal Control Standards	Risk Limits/Tolerance	Dynamic & Evolutionary
ERM Objective	Minimize Impact of Crisis	Meet Regulatory Requirements	Minimize Organizational Failures	Minimize Financial Loss	Maximize Stakeholder Value
Risk-Based Decisions	Crisis Solution	Compliance Focused: Policies & Procedures	Process & Operational Controls	Risk Transfer Strategies	Strategic & Business Decisions
Monitoring and Reporting	Ad Hoc Reporting	Regulatory Reporting	Audit & Internal Control Assessment	Static Dashboard	Continuous Dynamic Dashboards
Assurance and Effectiveness	Crisis Resolution	Regulatory Ratings/Feedback	Audit and Internal Control Rating	Policy Limit Conformance	Performance-Drive Feedback Loops

Diagram 4, Source: COSO-ERM2017

4.3 ERM Implementation Cycle

The basic cycle of the implementation begins with establishing the risk context and progresses through identification, analysis, evaluation, treatment, and monitoring/reviewing before returning to establishing context.

i. Communicate and Consult. Communicating with internal and external stakeholders at each stage in the process is central to this model.

ii. Establish the Context. Context includes business objectives, risk appetite, and criteria for evaluating risk.

iii. Identify Risks. Identify where, when, why, and how events could prevent, degrade, delay, or enhance the achievement of business objectives.

iv. Analyze Risks. Determine likelihood and consequences; identify and evaluate the effectiveness of existing controls.

v. Evaluate Risks. Prioritize risks by measuring them with the pre-established criteria and consider the potential benefits and adverse outcomes.

vi. Treat Risks. Develop and implement specific cost-effective strategies and action plans for increasing potential benefits and reducing potential costs.

vii. Monitor and Review. Monitor the effectiveness of the risk management program to ensure that it is operationally sound and cost-effective.

4.4 ERM Key Implementation Components *(Diagram 5)*

Diagram 5, Source: How to Communicate Risks Using Heat Maps, CGMA

5.0 RISK MEASUREMENT CRITERIA

5.1 Measurement of Risk Consequences

Conseq	Example Explanation	Value

uence	Financial Loss/ Opportunity Cost	Business Disruption	Reputation	Regulatory	Employee	
Catastrophic	Catastrophic Loss (>RM1,000k)	Greater than 1 week	Unable to Recover	Loss of listing/ licenses	Group wide low morale/ loss of key staff.	5
Major	Significant Loss (RM500k to <RM1,000k)	Up to 1 week	Recovery period up to 1 year	Public reprimand/ serious breach of stock exchange requirements	Significant spread of low morale/ increasing staff turnover	4
Moderate	Moderate Loss (RM250k to <RM500k)	Up to 48 hours	Recovery period up to 6 months	Private reprimand. Written warning by regulator/ stock exchange authorities	Localized low morale/ moderate staff turnover	3
Minor	Minor Loss (RM50k to <RM250k)	Up to 36 hours	Recovery period up to 3 months	Visit by local and enquiries by regulatory authorities	Low staff turnover	2
Insignificant	Insignificant Loss (<RM50k)	Up to 24 hours	Recovery period up to 1 month	Enquiries by regulatory authorities	Low level of dissatisfaction	1

5.2 Determine Likelihood

Likelihood	Example Explanation	Value
Almost Certain	High likelihood of occurrence unless controlled, i.e., almost certain to occur more than once within the next twelve months, e.g., past history	5
Likely	The risk is almost certain to occur within the next twelve months, unless controlled, e.g., past history	4

Moderate	Some likelihood of risk occurring unless controlled, i.e., the risk could occur at least once in the next 3 years	3
Unlikely	The risk could occur at least once in the next 3-5 years, e.g., past history in general industry and commerce	2
Rare	Very low potential for occurrence, e.g., unlikely to occur in the next 5 – 10 years	1

5.3 Assessing Impact

Impact	Rating	Description
5	Catastrophic	Loss of ability to sustain ongoing operations. An event or situation that would cause a stand-alone business to cease trading, e.g., • loss of significant (50% or more) production capability; • massive reduction in company credibility with shareholders, customers, suppliers, staff and public; • loss of key competitive advantage / opportunity; and • loss of supply of key process inputs.
4	Major	Reduced ability to achieve strategic objectives and targets, e.g., • sales/ revenue growth • market share • earnings per share • brand name/ reputation building Reduced ability to achieve business objectives, e.g., • loss of market confidence; • loss of key customers and sales opportunities; • short term (3 – 6 months) loss of production capability or distribution/ supply chains; • incurring excessive costs which impact ongoing profitability; • permanent reduction in product quality; and • loss or misappropriation of significant assets.
3	Moderate	Disruption to normal operations with a limited effect on achievement of corporate strategy and objectives, e.g., • temporary (less than 3 months) loss of production and distribution/ supply chains; • credibility damaged to some extent; • correctable product quality impact; and • loss of assets.

2	Minor	No material impact on the achievement of corporate strategy and objectives, e.g., • minor loss of production capability; • limited damage to reputation; • loss of audit trail; and • minor cost, quality and time impacts.
1	Insignificant	Accounting/administrative problems with no legal, decision-making or profit and loss impact.

5.4 Risk Matrix

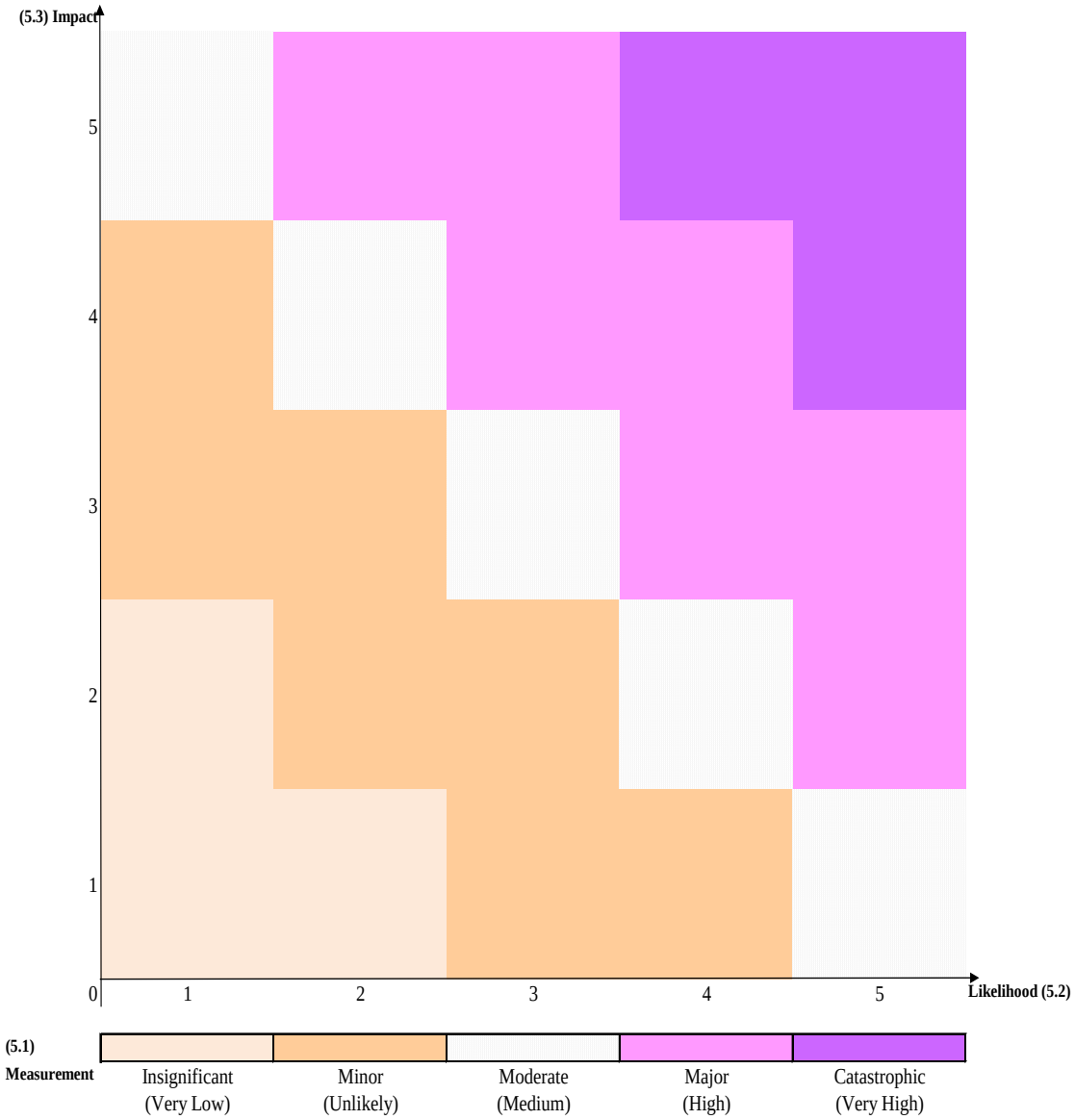

Diagram 6, Source: Measurement of Risk Matrix

6.0 ERM TECHNICAL TERMS

Risk

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.

Risk Control

Risk control is defined as any measures taken by a business to prevent, eliminate, or reduce losses; enhance the probabilities of gains; minimize the severity of losses that do occur or maximize gains.

Risk Event

A possible occurrence, which could affect (positively or negatively) the achievement of the investment objectives.

Risk Impact

The financial value of the effect of the risk event on one or more objectives, if it occurs.

Risk Likelihood

The chance (or probability) of the risk event occurring within a defined time period.

Risk Management

Risk management is a systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues.

Risk Management Process

Internal and external communication and continuous learning improve understanding and skills for risk management practice at all levels of an organization, from corporate through to front-line operations. The process provides common language, guides decision-making at all levels, and allows organizations to tailor their activities at the local level. Documenting the rationale for arriving at decisions strengthens accountability and demonstrates due diligence.

Risk Exposure

The likely loss or consequence of a risk. It is the combined probability and impact of a risk usually expressed as impacts.