DUOPHARMA

DUOPHARMA BIOTECH BERHAD

ENTERPRISE RISK MANAGEMENT FRAMEWORK

DUOPHARMA BIOTECH BERHAD | GROUP RISK MANAGEMENT & INTEGRITY

DUOPHARMA

GROUP RISK MANAGEMENT ("GRM") MISSION

Contribute to the creation, optimization and protection of company value through effective risk management

GRM OBJECTIVES

1. To promptly identify, measure, manage, report and monitor risks that affect the achievement of our strategic, operational and financial objectives.

2. To have a comprehensive risk management framework process to manage the principal risks we assume in conducting our business activities.

3. To create a comprehensive approach to anticipate, identify, prioritize, manage and monitor the portfolio of business risks impacting our organization.

4. To promote and inculcate a respectable enterprise risk management culture to contribute in the creation, optimisation and protection of value in the organization.

5. To ensure mitigation strategies continue to operate as intended and are modified as business conditions or risks change, in order to provide reasonable assurance.

CONTENTS

A. REVISION HISTORY

REV NO.	DATE	REVISION STATUS	PREPARED	REVIEWED	RECOMMENDED	APPROVED
R001	30 APR 2012	NEW	NM	LAAS	NOT APPLICABLE	DSAO
R002	13 FEB 2017	UPDATED INFORMATION	AE	LAAS	NOT APPLICABLE	DNAS
R003	03 APR 2018	UPDATED INFORMATION	AE	LAAS	NOT APPLICABLE	TSDPSSSB
R004	01 MAR 2019	UPDATED INFORMATION	AE	LAAS	DMRMY	TSDPSSSB
R005	10 DEC 2020	UPDATED INFORMATION	AE	LAAS	DMRMY	TSDPSSSB
R006	01 MAY 2023	UPDATED INFORMATION	WAN	LAAS	DMRMY	TSDPSSSB
R007	11 NOV 2024	UPDATED INFORMATION	WAN	LAAS	DMRMY	DPKAM

Abbreviations

AE = Anita Esa
DNAS = Dato' Normala Abdul Samad
DSAO = Dato' Sri Azalina Othman
DPKAM = Datin Paduka Kartini Abdul Manaf
DMRMY = Datuk Mohd Radzif Mohd Yunus
LAAS = Leonard Ariff Abdul Shatar
NM = Norzaimah Maarof
TSDPSSSB = Tan Sri Datuk Paduka Siti Sa'diah Sheikh Bakir
WAN = Wan Ahmad Nizam Wan Mohd. Salleh

B. DEFINITIONS / ABBREVIATIONS

The following terms and definitions apply for the purpose of this document.

Risk

Risk can be defined as the effect of uncertainty on Duopharma Biotech Group's objectives. Risk is generally associated with possible negative events and often characterized and expressed in terms of the likelihood of an event is occurring and its potential consequences.

Risk Management ("RM")

Risk Management is coordinated, continuous, proactive and systematic activities to identify, assess, manage, monitor and communicate risk from an organisation-wide perspective and to direct, control and mitigate Duopharma Biotech Group with regard to risk.

Enterprise Risk Management Framework ("ERMF")

ERMF sets out the policy, process, and guidelines for Duopharma Biotech Group's risk management practice, applicable across any business, functional, departments, product, process and project, and part of whole of the organisation.

1.0 PURPOSE

The purposes of an ERMF are as follows:

1.1 To establish a clear risk management policy and procedure.

1.2 To allocate and optimise the use of resources in managing risk effectively.

1.3 To inculcate an effective Risk Management culture throughout the Duopharma Biotech Group.

1.4 To establish an integrated risk management process where:

1.4.1 The risk management process within the organisation is formalised and key lines of responsibility for risk management throughout the Duopharma Biotech Group are defined;

1.4.2 Monitoring of major risk factors which may have a significant impact on Duopharma Biotech Group is carried out effectively; and

1.4.3 A transparent system of information and communication for risk management is achieved.

2.0 RISK MANAGEMENT POLICY

2.1 POLICY STATEMENT

It is the policy of the Duopharma Biotech Group of Companies to recognise the broad spectrum of risks which the Group faces along with the opportunities which it seeks in its businesses and operations. It is a strategic objective of the Group to have an effective risk management programme and control systems to assess and mitigate these risks and thereby facilitate the Group in meeting all its business objectives, most specifically:

2.1.1 To enhance the Group's high standards of corporate governance

2.1.2 To safeguard shareholder's investments

2.1.3 To safeguard the Group's assets

2.1.4 To develop the Group's employees and promote their well-being

2.1.5 To facilitate the Group's long-term growth under all business conditions

The Group is committed to developing and maintaining a risk management culture in its employees through leadership, education, communication and consultation so that a risk-based approach is effectively embedded in its business processes and operations.

2.2 RISK APPETITE

Risk appetite measures the amount and type of risk that the Group is willing to take or accept in the pursuit of its corporate and operational objectives. The risk appetite is reviewed yearly to align with the Group's budget and performance. Respective business unit is expected to operate within the thresholds defined in the risk appetite (refer to Appendix 1) and implement stringent measures when necessary.

3.0 SCOPE

The scope of activities for this enterprise risk management framework shall be extended to all of the Duopharma Biotech Group's operating levels and its subsidiaries. The scope shall be comprehensive to enable an effective and regular review of all high-risk activities, in order to safeguard the Duopharma Biotech Group's assets and shareholders' interests.

4.0 REFERENCE

The following documents are referred for the purpose of this framework:

4.1 ISO 31000: Risk Management – Principles and Guidelines

4.2 ISO 31000 Guide 73: Risk Management Vocabulary

4.3 IEC ISO 31010: Risk Assessment Techniques

4.4 Malaysian Code on Corporate Governance ("MCCG")

5.0 FRAMEWORK, GOVERNANCE, STRUCTURE AND RESPONSIBILITY

5.1 ENTERPRISE RISK MANAGEMENT FRAMEWORK

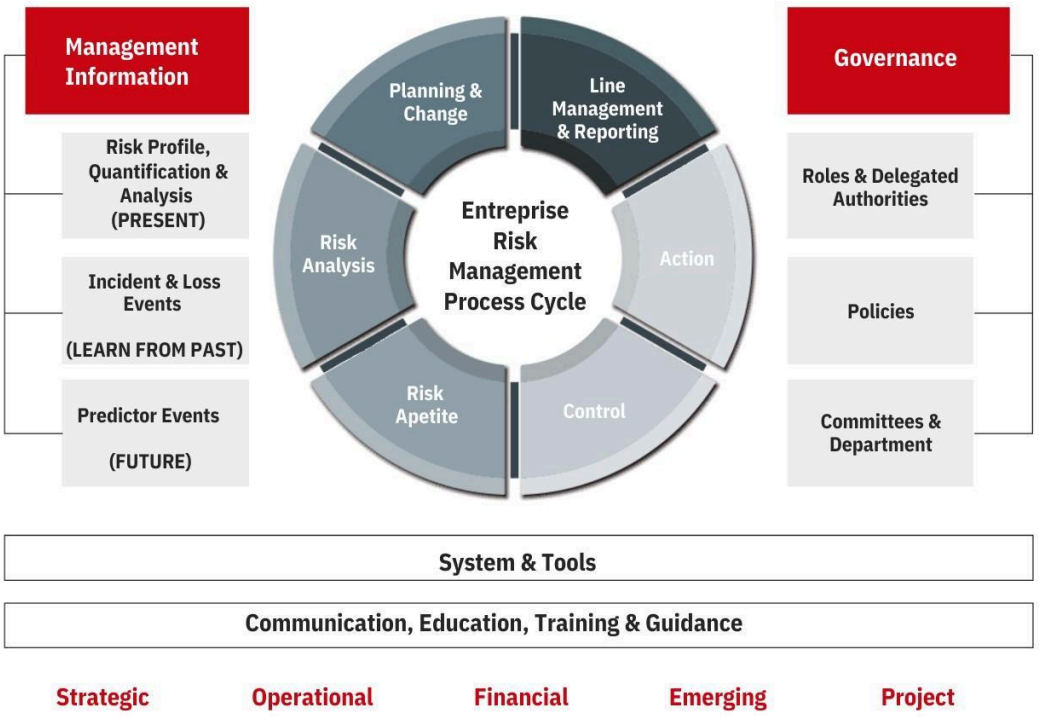


Figure 1: Enterprise Risk Management Framework

The Enterprise Risk Management Framework is aligned to the ISO 31000 Risk Management Principles and Guidelines. The framework defines the policy and objectives and sets the risk reporting structure. The framework structure includes risk profiling of current and historical risk information to anticipate probable future exposures. The framework ties into the Group's governance policies and guidelines via deliberations at various risk committees. The framework operates within the context of Key Risk Areas ("KRA"), but not limited to Strategic, Operational, Financial, Emerging and Project risks categories, but can be further expanded into several other categories such as Technological, Market, Environmental, Social & Governance ("ESG"), Cybersecurity, Climate-related etc. Within these broad categories, more specific risks that are associated to the risk categories have been identified. This approach enables the Group to effectively address evolving risk landscape such as Cybersecurity and Climate-related risk, and ensure the resilience of our business. For more detail on these key risk areas, please refer to Appendix 2.

5.2 RISK GOVERNANCE

Figure 2: Three Lines of Defence

The Group Risk Management & Integrity approach is premised on the Three Lines of Defence concept shown in ***Figure 2***. Under the Three Lines of Defence model, management control is the first line of defence, various established risk control and the compliance functions are the second line of defence while independent assurance is the third. Each of the three 'lines' play a distinct role within the governance framework. This model assists the achievement of objectives and facilitate strong governance and risk management places accountability and ownership, in ensuring an appropriate level of Independence and segregation of duties between Three Lines of Defence.

5.3 RISK MANAGEMENT STRUCTURE

The Risk Management Structure provides the framework used to assign responsibilities and facilitate the risk management process from transactional level to the Board of Directors ("BOD"), illustrated as follows:

Figure 3: Risk Management Structure

5.4 ROLES AND RESPONSIBILITY

The ultimate responsibility for managing Duopharma Biotech Group's risk rests with the BOD of the company. The BOD has instituted a stand-alone board Risk Management Committee ("RMC") at the BOD level to assist in the oversight of internal and exogenous risk factors that are surrounding the Group. This standalone RMC allows for more structured and focused oversight on risk matters.

Duopharma Biotech Group's risk management reporting structure follows the Risk Management Structure as described under ***Figure 3***. The in-house risk management function structure is subjected to any resolution of the BOD. The current risk management function reporting structure is as per Appendix 3.

5.4.1 RISK MANAGEMENT COMMITTEE ("RMC")

The purpose, compositions, appointment of members and duties of RMC is presented in the table below:

PURPOSE

- To assist the BOD in ensuring that there is a sound system for risk management and effective oversight of investment, integrity and whistleblowing practices within the Company and its subsidiaries (collectively referred to as "Group"); and
- In the exercise of its functions, it is understood that the RMC is not delegated with decision making powers but shall report its recommendations to the Board for decision. The existence of the RMC does not diminish the Board's ultimate statutory and fiduciary responsibility for the decision-making relating to the functions and duties of the Committee.

COMPOSITION

- Size
  - The committee shall have at least (3) members.
- Membership
  - The Committee shall comprise a majority of independent Directors; and
  - The Chairman of the Board shall not be a member of the Committee
- Chairman of the Committee
  - The Chairman of the Committee shall be a Non-Executive Director; and
  - Before appointment as Chairman of the RMC, it is desirable for the appointee to have served on the RMC for an appropriate period.
- Secretary of the committee
  - The secretary of the Committee ("Secretary") shall be the Company Secretary or his representative.

APPOINTMENT OF MEMBERS

- The Nomination and Remuneration Committee shall recommend the appointment of RMC members to the Board;
- Members shall be appointed based on their ability to devote time, skills and experience relevant to their duties within the RMC; and
- The members serving the RMC shall be changed at appropriate and regular intervals. In order to ensure that the entire Committee is not replaced at any one time, such change of members shall be done on a progressive basis.

5.4.1 RISK MANAGEMENT COMMITTEE (RMC) (Con't)

DUTIES

Subject to any resolution of the Board, the duties of the Committee are to:

•To carry out the following, in relation to the **risk oversight**:

(a) Determine the Group's risk appetite, framework, policies and processes for identifying and managing and/or accept risks beyond the approval discretion provided to Management.

(b) Provide recommendations to the Board on the risk strategy, parameters of the Group's risk reward trade-off, monitor the alignment of the Group's risk profile with the risk appetite and ensure that the Group maintains an appropriate level and quality of capital in line with the risks inherent in its activities and projected business performance;

(c) Monitor changes anticipated for the business environment, including consideration of emerging risks, legislative or regulatory changes, major initiatives and other factors considered relevant to the Group's risk profile and provide report on the same to the Board for overall consideration on the Group's business and operations;

(d) Engage Group Risk Management and Integrity Department ("GRMI") in ongoing risk appetite dialogue and provide timely input to the Senior Management as business condition changes and new opportunities arise;

(e) Receive, review, scrutinise and provide commentaries on reports from the GRMI concerning:
i) Risk management policies, strategies, processes and controls, status of the implementation and effectiveness thereof, within the divisions and, if thought fit, approve or vary them;
ii) Alignment or integration of risk management activities with other management activities/tools which include formulation of strategies, development of business plans, budgeting, forecasting and performance review, within the divisions; and
iii) Identification, management and mitigation of enterprise risks which could impact the achievement of business objectives.

(f) Encourage a healthy risk culture and watch for dysfunctional behaviours which may impair the effectiveness of the risk management process;

5.4.1 RISK MANAGEMENT COMMITTEE (RMC) (Con't)

DUTIES (Con't)

(g) Review and recommend to the Board the policies and procedures for managing risks within the Group, including assessing information technology and cybersecurity risks;

(h) Review and recommend to the Board the statement on risk management and internal control;

(i) Review the external auditor's management letter and management's response;

(j) Identifying and monitoring the Group's corruption risks;

(k) Approve and report the same to the Board the appointment and termination of the Head of GRMI;

(l) Review the job grade of the Head of GRMI;

(m) Review the adequacy of resources allocated for effective management of risk within the Group;

(n) Overseeing the GRMI so as to ensure it is carried out by the right personnel with the skills, experience, training and authority; and

(o) Oversee disclosures relating to risk management in accordance with Main Market Listing Requirements ("MMLR") of Bursa Malaysia Securities Berhad and the MCCG.

5.4.1 RISK MANAGEMENT COMMITTEE (RMC) (Con't)

DUTIES (Con't)

• To carry out the following, in relation to the **investment oversight**:

(a) Approve and report the same to the Board considerations relating to proposed investments (including mergers and acquisitions) for investment which is not regarded as Related Party Transaction for consideration/value of assets equal or up to USD 1.0 million.

(b) Review and recommend to the BOD all budgeted capital expenditure in excess of RM3.0 million as proposed by companies within the Group;

(c) Review and recommend to the BOD all acquisition of assets/properties (including land and trademarks) by the Group. *Note: The Group Managing Director ("GMD") is given the authority to approve any budgeted capital expenditure (excluding land and properties) amounting to RM3.0 million and below, in line with the Group's Limits of Authority. All capital expenditure approved by the GMD shall be tabled to the RMC for information*;

(d) Approve up to RM 5.0 million unbudgeted operating expenditure item exceeding the GMD's limits of authority up to a maximum of RM1.0 million and report the same to the Board;

(e) Review and recommend to the Board unbudgeted operating expenditure item exceeding RM 5.0 million;

(f) Review and recommend to the BOD all acquisitions, investments and divestments of companies (excluding dormant companies), setting up of new business including joint ventures, irrespective of value, and disposal of business;

(g) Monitor progress of investment proposals, capital expenditure and projects approved by the BOD;

(h) Approve unbudgeted capital expenditure of up to RM 1.0 million and report the same to the Board;

(i) Review and recommend to the BOD unbudgeted capital expenditure exceeding RM 1.0 million;

(j) Review the post-expenditure review of the investment proposal, capital expenditures and projects approved by the RMC and the BOD (as the case maybe) at least eighteen (18) months upon commencement of the projects; and

(k) Reviewing financial and operational performance of investments or projects against projected returns.

5.4.1 RISK MANAGEMENT COMMITTEE (RMC) (Con't)

DUTIES (Con't)

• To carry out the following, in relation to the **integrity oversight**:

(a) Review and recommend to the Board all matters related to the governance of integrity/anti-corruption within the Group.

(b) Review annually:

- the Group's business ethics and integrity policies and to make recommendations to the Board thereon; and
- the Group's business ethics and integrity processes and practices

(c) Monitor the responses to the Group's whistleblowing line and other mechanisms used to raise concerns, and to oversee actions following breaches of the ethics and business integrity policy or allegations of misconduct;

(d) Review the whistleblowing preliminary evaluation and findings relating to integrity/anti-corruption matters and assess whether a detailed investigation is warranted pursuant to the completion of the preliminary evaluation by the Integrity Office;

(e) Review and recommend to the Board the policies and practices of the Group in respect of business ethics and integrity in relation to the commencement of operations in any new country or territory in which the Group has not previously operated;

(f) Review and recommend to the Board, compliance with particular best practice guidance or codes in relation to business ethics, integrity and compliance;

(g) Review the implementation and monitoring of the Group's ISO 37001:2016 Anti-Bribery Management System; and

(h) Ensure that the Group's communication and training programmes on ethics and business integrity are effective in reinforcing ethical values and further enhance good corporate governance.

5.4.2 EXECUTIVE RISK MANAGEMENT COMMITTEE ("ERMC")

The purpose, compositions, appointment of members and duties of ERMC is represented in the table below.

PURPOSE

- To assist the RMC in ensuring that there is a sound system for an effective risk management within the Company and its subsidiaries.

COMPOSITION

- Consists of the Group Management Committee members. The Chairman of the Committee is the GMD.

APPOINTMENT OF MEMBERS

- Not applicable.

DUTIES

- Recommend to the RMC the risk appetite, frameworks, policies and processes for identifying and managing risk and highlight the risks that are beyond the approval discretion provided to Management.
- Deliberate the management of strategic, financial, operational and projects risks which could impact the achievement of business objectives.

5.4.2 EXECUTIVE RISK MANAGEMENT COMMITTEE (ERMC) (Con't)

DUTIES (Con't)

- Monitor changes anticipated for the business environment, including consideration of emerging risks, legislative or regulatory changes, major initiatives and other factors considered relevant to the Group's risk profile and provide report on the same to the RMC for overall consideration on the Group's business and operations.
- Recommend to RMC risk appetite to suit changes in business condition and exploration of new opportunities.
- Receive, review, scrutinise and provide commentaries on reports from the GRMI concerning:

  (a) Risk management policies, strategies, processes and controls status of the implementation and effectiveness thereof, within the divisions and, if thought fit, approve or vary them;

  (b) Alignment or integration of risk management activities with other management activities/tools which include formulation of strategies, development of business plans, budgeting, forecasting and performance review, within the divisions; and

  (c) Identification and management of enterprise risks which could impact the achievement of business objectives.
- Establish a robust and sustainable risk management culture within the organization.
- Oversee disclosures relating to risk management and sustainability in accordance with MMLR of Bursa Malaysia Securities Berhad and the MCCG.

5.4.3 RISK CHAMPION

The purpose, compositions, appointment of members and duties of Risk Champions (refer to Appendix 4) is represented in the table below.

PURPOSE

- Responsible for managing the risks in the respective department or area of responsibility.

COMPOSITION

- Consists of all Heads of Departments and Senior Managers for departments without Heads.

APPOINTMENT OF MEMBERS

- The Chief of the relevant department shall recommend the appointment of Risk Champions.
- The appointment is based on their position as heads of department or role of managing a group of people.

DUTIES

- To ensure the application of risk appetite, frameworks and policies and processes when identifying and managing risk in the department or area of responsibility.
- Deliberate the management of strategic, financial, operational and projects risks which could impact the achievement of department or area under responsibility's objectives and ensure that sufficient budget is available to perform effective risk management.

5.4.3 RISK CHAMPION (Con't)

DUTIES (Con't)

- Monitor changes anticipated for the business environment, including consideration of emerging risks, legislative or regulatory changes, major initiatives and other factors considered relevant to the department and area under responsibility's risk profile and provide report on the same to the ERMC for overall consideration on the Group's business and operations.
- Implement and propose risk appetite to ERMC to suit changes in business condition and exploration of new opportunities.
- Receive, review, scrutinise and provide commentaries on risk profile from risk owners concerning.

  (a) Risk management processes and controls, status of the implementation and effectiveness thereof, within the department and area of responsibility and, if thought fit, approve or vary them;

  (b) Alignment or integration of risk management activities with other management activities/tools which include formulation of strategies, development of department plans, budgeting, forecasting and performance review, and

  (c) Identification and management of enterprise risks which could impact the achievement of department and area of responsibility's objectives.

  (d) Review internal and external audit reports to identify issues related risks.
- Review, scrutinise and provide commentaries on risk assessment reports for proposed investments (including mergers and acquisitions), strategic plans as well as key performance indicators;
- Ensure that risk management is a regular agenda in the department meetings with the objective to embed risk culture in the department.

5.4.4 RISK COORDINATOR

The purpose, compositions, appointment of members and duties of Risk Coordinator is represented in the table below.

PURPOSE

- To assist Risk Champion in managing risk within the department or area of responsibility.

COMPOSITION

- Consists of selected Manager in the respective department.

APPOINTMENT OF MEMBERS

- The Risk Champion shall recommend the appointment of Risk Coordinator.
- The appointment is based on their ability to influence and gain support from risk owners.

DUTIES

- To assist Risk Champion in the application of risk appetite, frameworks and policies and processes when identifying and managing risk in the department or area of responsibility.
- Assist Risk Champions to deliberate the management of strategic, financial, operational and projects risks which could impact the achievement of department or area under responsibility's objectives within the approved budget.

5.4.4 RISK COORDINATOR (Con't)

DUTIES (Con't)

- Update Risk Champions to monitor changes anticipated for the business environment, including consideration of emerging risks, legislative or regulatory changes, major initiatives and other factors considered relevant to the department and area under responsibility's risk profile and provide report on the same to the ERMC for overall consideration on the Group's business and operations.
- Update Risk Champion on feedback from Risk Owners on changes in the department and area under responsibility.
- Assist Risk Champion to obtain required information for effective assessment of risk status in the department or area under responsibility.
- Assist Risk Champion on risk assessment reports for proposed investments (including mergers and acquisitions), strategic plans as well as key performance indicators;
- Support and assist the Risk Champion and GRMI in the implementation of Risk Management programs.

5.4.5 RISK OWNER

The purpose, compositions, appointment of members and duties of Risk Owner is represented in the table below.

PURPOSE

- Responsible for managing the risks in the respective area of responsibility.

COMPOSITION

- All Duopharma Biotech Group staff.

APPOINTMENT OF MEMBERS

- Not applicable

DUTIES

- Identify and manage risks within the area of responsibility.
- Ensure the appropriate controls and treatment plans are in place to manage identified risks within the approved budget.
- Monitor and report the implementation and effectiveness of controls and treatment plans.
- Perform the risk assessment and review of the effectiveness of controls and treatment plans against changes in area of responsibility.
  (a) Update the risk profiles in particular the progress of the risk mitigation plan implementation, the adequacy and effectiveness of existing controls as well as the current residual risk exposure for the identified risks.
  (b) Review internal & external audit reports in order to identify issues related risks.
  (c) Ensure that full consideration and commentary on risk control and treatment plans are provided to support department strategy and plans.
- Perform the risk assessment and deliberate the effectiveness of controls and treatment plans against proposed investments (including mergers and acquisition), strategic plans as well as own key performance indicators.
- Perform risk management on day-to-day basis and participate in GRMI risk management programs.

6.0 RISK MANAGEMENT PROCESS

The following diagram describes the risk management process adopted by Duopharma Biotech Group based on the ISO 31000 Risk Management Principles and Guidelines:

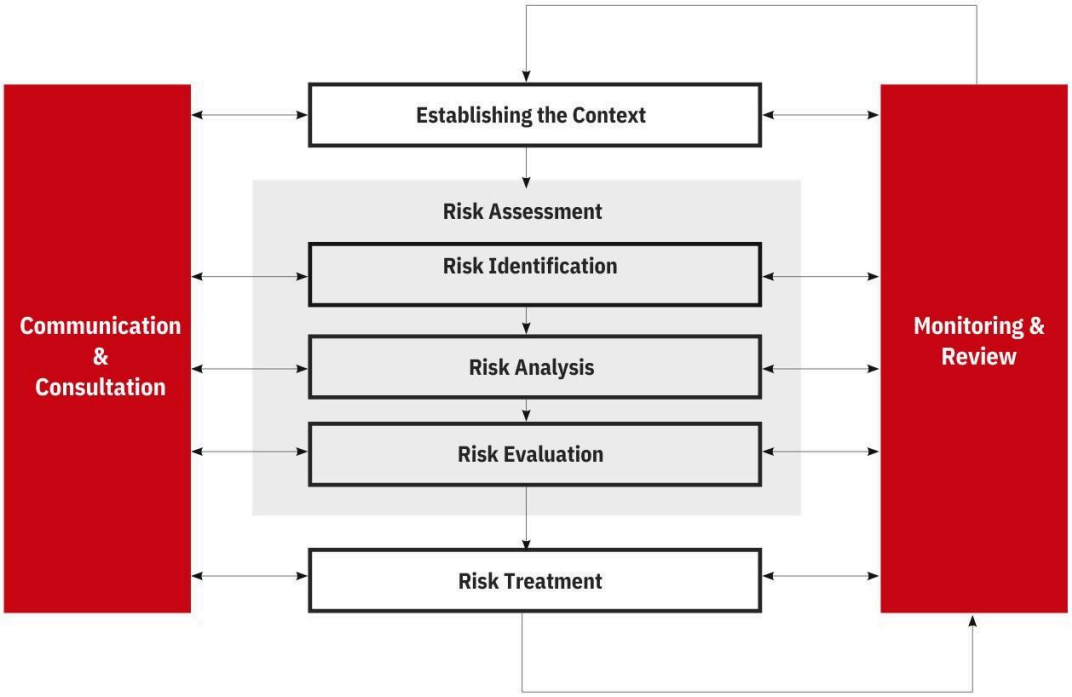


Figure 4: Risk Management Process

6.1 ESTABLISHING THE CONTEXT

It is essential to establish the right context when managing risk by defining the Group's most important external and internal parameters. The Group's external context includes its external stakeholders, its local, national, and international environment, as well as any external factors that influence Duopharma Biotech's objectives. Duopharma Biotech's internal context includes its internal stakeholders, approach to governance, contractual relationships, capabilities, culture, and standards. Examples of key areas for external and internal contexts for the risk management process in Duopharma Biotech are listed in Appendix 2.

6.2 COMMUNICATION AND CONSULTATION

Communication and consultation of risk are key elements in managing risk in Duopharma Biotech. It must be continual, iterative, and two-way process that involves both sharing and receiving of information in the management of risk. Duopharma Biotech shall establish decisions and directions that the Group will pursue based on the communication and consultation of the risks in terms of the existence of risks, their nature, form, likelihood, and significance, as well as whether or not risks are acceptable or should be treated, and what treatment options should be considered.

6.3 RISK ASSESSMENT

The risk assessment involves three key steps; Risk Identification, Risk Analysis and Risk Evaluation and these processes are described as follow;

6.3.1 RISK IDENTIFICATION

Risk Identification is the process of identifying and describing the potential or actual risk events. The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. Comprehensive identification is crucial because a risk that is not identified at this stage will not be included in further analysis. Key components when identifying a risk event shall include:

- The objective
- Name and description risk events
- Causes of the risk events
- Consequences of the risk events (financial and non-financial)
- Areas of impacts

Risks are identified using a combination of Top-Down and Bottom-Up approaches. In the Top-Down approach, risks are identified at the Group level highlighting key risk within respective key risk areas which are residually significant and impacting the Group under the present environment over short, medium and long-term horizons. The Bottom-Up approach on the other hand, begins at the lower levels of the organization and progresses upward, effectively capturing mainly operational risks that may affect specific departments and functions. This dual approach provides a comprehensive view of both strategic and operational risks across the Group.

6.3.2 RISK ANALYSIS

Risk Analysis involves developing an understanding of the risk. Risk analysis provides an input to risk evaluation and decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods. Risk is analyzed by determining its consequences and likelihood, and compare it to the established and approved Risk Criteria and Risk Matrix.

6.3.2.1 RISK CRITERIA

Risk Criteria are the references used to evaluate the significance or importance of an organization's risks. They are used to determine whether a specified level of risk is acceptable or tolerable (Risk Appetite). Risk criteria should reflect organization's values, policies, and objectives, should be based on its external and internal context, should consider the views of stakeholders, and should be derived from standards, laws, policies, and other requirements.

The Group's risk criteria in terms of consequence and likelihood scale are as per Appendix 5. The risk criteria shall be cascaded down to all levels to ensure the risk analysis is accurate in addressing the weight of a particular risk event.

6.3.2.2 RISK HEAT MAP

Risk Heat Map is a risk matrix that is used for graphical representation of the severity of a particular risk event. Duopharma Biotech adopted 5 by 5 risk heat map to capture risk identified by risk owners as per Appendix 6, to represent the likelihood and consequence of a risk event, applicable to rank the gross, residual and target risk ratings.

6.3.3 RISK EVALUATION

Risk Evaluation is the process to evaluate the residual risk level of a particular risk event, by assessing the effectiveness of the current internal controls in place to mitigate the risk. If the residual risk level has yet to achieve the desired or targeted risk level, inadequacy of controls must be addressed by planning an appropriate management action or treatment plans to treat the risk. The steps in a risk evaluation process are shown in the diagram below:

Figure 5: Evaluation Process

Generic guidelines in assessing the controls effectiveness and definition of gross, residual and target risk ratings are as per Appendix 7 and 8.

6.4 RISK TREATMENT

Risk Treatment involves selecting one or more options/mitigation strategies for modifying the likelihood and consequences of risk events, and implementing those options/mitigations strategies.

6.4.1 RISK RESPONSE – RISK DECISION

There are four options of risk responses when considering a risk treatment plan. Decisions on whether further actions required involve:

RISK DECISION	DESCRIPTION
Accept	No action is required to affect likelihood or consequences. If risk Decision is to accept, then no Risk Treatment is required and the Targeted Risk Level will be the same as Residual Risk Level.
Avoid	Exiting the activities giving rise to the event. This may involve exiting a product Line, declining expansion to a new geographical market or selling a division.
Transfer	Action taken to move the risk event to a 3rd party - full transfer or sharing some part of the risk. It is important to note that transfer of risk does not result in transfer of accountability, the risk owner will remain accountable. Transfer the risk by purchasing insurance or similar products that cover business interruption. Guarantees some degree of financial stability. Provides time to recover while maintaining business accounts. May not cover every type of disaster due to cost prohibitive.
Treat	Action taken to reduce likelihood or consequences of both.

6.5 MONITORING AND REVIEW

Both monitoring and review should be a planned part of the risk management process and involve regular checking and surveillance which can be periodic or ad hoc.

6.5.1 RISK REVIEW AND REPORTING

Planned risk review sessions will be conducted by GRMI to review the risk registers on quarterly basis prior to RMC reporting and meeting. The review sessions shall discuss the progress of risk controls and treatment plans in place, and the residual risk levels of every risk event, upon the execution of control and treatment plan. Subsequent to the review sessions, updated risk reports will be consolidated by GRMI for the issuance of quarterly risk reports to and RMC.

7.0 RISK MANAGEMENT TOOLS

7.1 DILIGENT ONE (formerly known as HIGHBOND)

The Group utilizes an online ERM system, namely 'Diligent One' or previously known as 'HighBond', to ensure efficient, consistent and accurate risk management reporting. Diligent One is the platform for the risk management process to be documented, reviewed and updated, and all information gathered in the system shall be the key reference for any analysis of the company risk profile. All risk owners, risk coordinators and related personnel shall have access to Diligent One with dedicated username and password.

7.2 RISK ASSESSMENT WORKSHOPS

Formalized Risk Assessment Workshop is part of the risk management activities for the Group. GRMI will be key driver of the program and supported by Risk Champions. Formal Risk Assessment modules shall be prepared prior to the workshop to define the scope and coverage of the assessment by reviewing existing Key Risk Areas and pre-identifying new Key Risk Areas for the department. The assessment will be carried out upon approval of the modules by the Management, the results and findings of the risk assessment will be reported to ERMC and RMC and upon approval, the risk will be registered in the Diligent One for further monitoring and updates. ***Figure 6*** describes the process for a Risk Assessment Workshop:

Figure 6: Risk Assessment Workshop

7.3 RISK ASSURANCE

Quarterly and yearly assurance are provided by the GMD and Chief Financial Officer to the RMC that all risks to the best knowledge of all stakeholders are identified, addressed and reviewed. The Senior Management Team provides quarterly assurance to the GMD on the said matters.

7.4 SOURCES OF INFORMATION

Internal Audit reports, monthly operations reports, weekly market monitoring report, safety reports and other relevant reports shall be the additional sources of information to ensure appropriate coverage of risk management across the organization.

8.0 REVIEW & REVISION

GRMI will review this ERMF periodically to be in line with current practices and guide. All revisions or amendments to this ERMF as recommended by the GRMI shall be reviewed by the ERMC, and subsequently for the RMC's endorsement and recommendation for the BOD's consideration and approval.

9.0 APPENDICES

APPENDIX 1: RISK APPETITE

APPENDIX 2: KEY RISK AREAS

APPENDIX 3: RISK MANAGEMENT REPORTING STRUCTURE

APPENDIX 4: LIST OF RISK CHAMPIONS

APPENDIX 5: LIKELIHOOD SCALE

APPENDIX 6: RISK RATING HEAT MAP

APPENDIX 7: CONTROL EFFECTIVENESS RATING DEFINITION

APPENDIX 8: RISK RATING DEFINITION

APPENDIX 9: AWARDS & ACHIEVEMENT

APPENDIX 10: CONTACT

APPENDIX 1: RISK APPETITE

PARAMETER	SEVERITY (CONSEQUENCES)				
	NEGLIGIBLE	LOW	MEDIUM	MAJOR	CATASTROPHIC
Earnings at Risk (RM 'mil)	< 1.2%	1.2% - 2.5%	2.5% - 3.8%	3.8% - 5.0%	> 5.0%
	1.0	1.0 2.2	2.2 3.3	3.3 4.3	4.3
CAPEX at Risk (RM 'mil)	< 1.2%	1.2% - 2.5%	2.5% - 3.8%	3.8% - 5.0%	> 5.0%
	<2.6	2.6 5.4	5.4 8.2	8.2 10.9	>10.9
OPEX at Risk (RM 'mil)	< 1.2%	1.2% - 2.5%	2.5% - 3.8%	3.8% - 5.0%	> 5.0%
	<2.8	2.8 5.9	5.9 9.0	9.0 11.8	>11.8
OTIF (Overall)	≥ 95%	85% to 95%	80% to 85%	70% to 80%	< 70%
OTIF (Finished Goods Warehouse)	≥ 97.5%	95% to 97.5%	92.5% to 95%	90% to 92.5%	< 90%
Key IT Infrastructure Unplanned Downtime	< 2 hours non-operational	2 hours to 12 hours non-operational	0.5 day to 1 day non-operational	1 day to 1.5 days non-operational	>1.5 days non-operational
Key IT Application Unplanned Downtime	< 2 hours non-operational	2 hours to 12 hours non-operational	0.5 day to 1 day non-operational	1 day to 1.5 days non-operational	>1.5 days non-operational
Regulatory / Legal / Compliance	Isolated non-compliance ; Negligible financial and non-financial impact (reputation, customer confidence etc.).	Contained non-compliance resulting in reprimands and some impact on normal operations; Minor financial and non-financial impact.	Significant non-compliance resulting in reprimands and fines; Moderate financial and non-financial impact.	Major non-compliance resulting in reprimands and fines; Adverse financial and non-financial impact.	Extensive non-compliance resulting in potential prosecution; Shutdown of business operations.
Reputation / Image	Minimal / no impact on image / reputation.	Potential impact on image / reputation.	Image / reputation will be affected in the short term.	Serious impact with potential for permanent diminution in image / reputation with adverse publicity.	Sustained, serious loss in image / reputation in the longer term.

PARAMETER	SEVERITY (CONSEQUENCES)				
	NEGLIGIBLE	LOW	MEDIUM	MAJOR	CATASTROPHIC
Safety	Near misses. Unsafe condition and unsafe act.	First aid required.	Injury involving medical treatment or hospitalisation resulting in loss time.	Significant injury involving medical treatment or hospitalisation resulting in lost time and DOSH reportable.	Serious long-term injury. Individual fatality or extensive long-term injury with potential permanent disability.
	TRCF < 0.3	TRCF = 0.3 – 0.5	TRCF = 0.5 – 1.3	TRCF = 1.3 – 5.0	TRCF more than 5.0
Environmental & Natural Hazard	Isolated hazards at one site that interrupted operation <1 day	1. Minimal physical impact at one site that interrupted operations not more than 3 days. 2. Business Continuity Management (BCM)'s incident / crisis severity - Code Green.	1. Minor physical impact at one site that interrupted operations not more than 5 days. 2. Hazards contained within internal resources. 3. BCM's incident / crisis severity - Code Amber.	1. Significant physical impact at all sites that interrupted operations up to 2 weeks. 2. Partial accessibility to sites. 3. Require external resources to contain hazards. 4. BCM's incident / crisis severity - Code Amber.	1. Significant physical impact at all sites that interrupted operations more than 2 weeks. 2. Access to sites completely denied. 3. Managed by external services. 4. Long term remediation required. 5. BCM's incident / crisis severity - Code Red.
Human Capital Management	Succession planning for Direct Report 1 Zero (0) position. Regrettable resignation One (1) HIPOT.	Succession planning for Direct Report 1 One (1) position. Regrettable resignation Two (2) HIPOT.	Succession planning for Direct Report 1 Two (2) positions. Regrettable resignation Three (3) HIPOT.	Succession planning for Direct Report 1 Three (3) positions. Regrettable resignation Four (4) HIPOT.	Succession planning for Direct Report 1 More than Three (3) positions. Regrettable resignation More than Four (4) HIPOT.

Human Capital Management	No variance from EEI target	0-10% negative variance from target EEI	10-20% negative variance from target EEI	20-30% negative variance from EEI	>30% negative variance from EEI
Cybersecurity	Impact to individual user data or documents, with self-quarantine. The recovery time is not more than 96 hrs	Impact only at user's device, with self-quarantine in control. The recovery time is not more than 72 hrs	Impact only to whole department / individual user operation with quarantine in control. The recovery time is not more than 48 hrs for department.	Impact only to whole business unit operation with quarantine in control. The recovery time is not more than 24 hrs	Impact whole Group business operation. Disaster Recovery Plan in control, with recovery time of objective "RTO" is not more than 12 hrs for 1st priority system "SAP", 2nd priority system is not more then 24hrs.

PARAMETER	SEVERITY (CONSEQUENCES)				
	NEGLIGIBLE	LOW	MEDIUM	MAJOR	CATASTROPHIC
Bribery & Corruption	1. No conflicts with any engaged stakeholders. 2. Minor breach of internal process and controls.	1. Some adverse publicity. 2. Minor loss of stakeholder confidence. 3. Internal review of existing policies and practices instigated. 4. Breach of SOP.	1. Substantial adverse publicity. 2. Loss of some stakeholder confidence. 3. Risk event requires Management response. 4. Breach of ABAC Policy	1. Adverse national media reports on failing, inefficiency or inadequacy. 2. Serious loss of stakeholder confidence 3. Serious consequences to Senior Management which may lead to penalty / imprisonment. 4. Breach of applicable laws (MACC Act, Prevention of Corruption Act, Corruption Eradication Law) and regulations resulting in penalty.	1. Intense public, political and media scrutiny / criticism evidenced, adverse international media and reports / sustained media coverage. 2. Complete loss of stakeholder confidence. 3. Board of Directors faces penalty / imprisonment. 4. Breach of laws and regulations resulting to criminal penalty.

OTIF = On Time in Full
EEI = Employee Engagement Index
TRCF = Total Recordable Case Frequency
HPOT = High Potential Employee

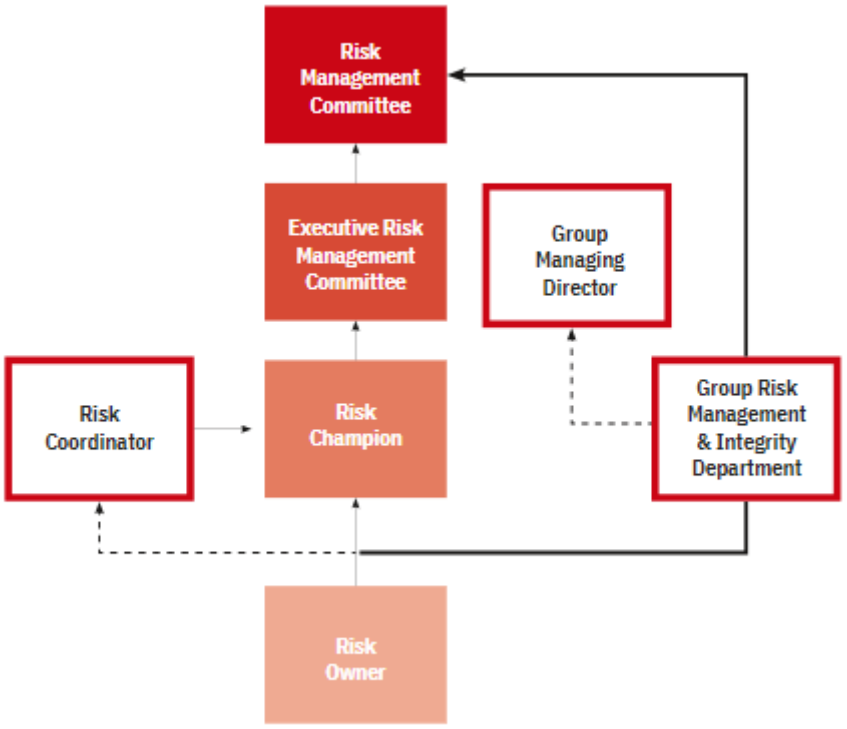
APPENDIX 2: KEY RISK AREAS

RISK CATEGORIES	DESCRIPTION
Strategy	Risk associated with the Group strategic directions including diversifying into renewable energy and green technologies.
Financial	Risk associated with revenue leakages, liquidity, cashflow management, capital planning, budgeting, and loans and receivables management.
Environment, Social and Governance	The risk of uncertainty in sustaining the growth and/or maintaining a sound and effective sustainable system due to industrial or commercial activities. ESG risks include those related to climate change impacts mitigation and adaptation, environmental management practices and duty of care, working and safety condition, respect for human rights, anti-bribery and corruption practices, and compliance to relevant laws and regulations.
Legal/ Regulatory	Risks arising from non-compliance to laws and relevant regulatory requirements.
Operational	Risk associated with operational matters, including additional new business divisions, functions and/ or activities such as work process, limited resources, planning & timeline, testing, machine & equipment and maintenance.
Reputation/ Media	Risk arising due to negative publicity within social media (e.g. news, opinion articles, social media posts, reputation index or customer complaints).
Bribery and Corruptions	Risk arising due to bribery and corruptions detected by internal or external regulators/ auditors.
Health and Safety	Potential significant workers and/or third party's compensation liabilities (civil and criminal), fatalities, incompliance with the Safety and Health requirements, damage to the business reputation and/or any other events occurring due to hazardous working conditions.
Technology	Technology risks typically manifest with the development and use of emerging technologies such as renewable energy, battery storage, energy efficiency, and carbon capture and storage. This affects the competitiveness of our businesses through areas such as operational costs, and ultimately demand for our services from end clients. To the extent that new technology displaces old systems and disrupts some parts of the existing economic system, winners and losers will emerge from this “creative destruction” process.

RISK CATEGORIES	DESCRIPTION
Cybersecurity	The Company recognizes the critical importance of cybersecurity in safeguarding its operations, intellectual property, and sensitive data. As such, cybersecurity is integrated into the Company's overall risk management framework. A robust cybersecurity management is in place to identify, assess, mitigate, and monitor cyber risks across the Company's operations, including Malaysia, Singapore, Indonesia and Philippines. The cybersecurity management encompasses a comprehensive range of measures, including: • **Risk Assessment**: Regular evaluation of potential cyber threats and vulnerabilities to identify critical assets and prioritize mitigation efforts. • **Operational Efficiency:** These measures include automating routine tasks, upgrading collaboration tools, providing regular cybersecurity training to employees, and using data analytics to make informed decisions. • **Infrastructure Enhancement:** This includes ensuring that hardware and software are up-to-date to maintain a secure environment, as well as implementing robust data backup and recovery procedures to minimize the impact of potential incidents. • **Preventive Measures:** Implementation of robust technical controls, such as endpoint security, network segmentation, regular security audits and third-party validation. • **Compliance:** Adherence to relevant cybersecurity regulations and industry best practices. The Company maintains ongoing monitoring and evaluation of its cybersecurity posture to adapt to the evolving threat landscape.

RISK CATEGORIES	DESCRIPTION
Climate - related	Duopharma Biotech is committed to transitioning to a low-carbon economy and recognizes the critical importance of climate risk management. Climate change considerations have been integrated into our governance structure, with the Board overseeing climate risk mitigation strategies as part of our 5-Year ESG Strategy. Key elements of our climate risk management strategy include: • **Comprehensive Risk Identification:** We have conducted a thorough assessment of potential climate-related risks across our operations in Malaysia, the Philippines, Singapore, and Indonesia. These risks include both physical risks (e.g., extreme weather events, rising sea levels) and transition risks (e.g., policy changes, technological advancements). • **Risk Prioritization and Management**: Identified risks have been prioritized and registered in our ERM system for ongoing monitoring and review. We have developed and implemented mitigation strategies to reduce our exposure to these risks. • **Investment in Mitigation Initiatives:** To mitigate climate change risks, we have allocated budgets for initiatives such as renewable energy (e.g., solar panels) and water conservation measures

APPENDIX 3 : RISK MANAGEMENT REPORTING STRUCTURE



APPENDIX 5 : LIKELIHOOD SCALE

LIKEHOOD SCALE		
Level	**Description**	**Probability (P) of Occurence in a year**
Rare	Event may occur only in exceptional circumstances	P ≤ 5%
Unlikely	Event could occur at some time	P ≤ 20%
Possible	Event might occur at some time	P ≤ 50%
Likely	Event will probably occur only in most circumstances	P ≤ 80%
Almost Certain	Event is expected occur only in most circumstances	P > 80%

APPENDIX 6 : RISK RATING HEAT MAP

SCORE			Severity (Consequences)				
			1 Negligible	2 Low	3 Medium	4 Major	5 Catastrophic
Frequency (Likelihood)	5	Almost Certain	High 11	High High 16	Extreme 20	Extreme 23	Extreme 25
	4	Likely	Moderate 7	High 12	High High 17	Extreme 21	Extreme 24
	3	Possible	Minor 4	Moderate 8	High 13	High High 18	Extreme 22
	2	Unlikely	Trivial 2	Moderate 5	Moderate 9	High 14	High High 19
	1	Rare	Trivial 1	Minor 3	Moderate 6	High 10	High High 15

No.	Matrix Score	Requirement	
		Appropriate Control Response	Monitoring & Review
1.	Trivial	▪ Accept the risk.	▪ Notation and reporting.
2.	Minor	▪ Manageable by implementing new or with the current routine controls and procedures.	▪ Yearly periodic review and monitoring.
3.	Moderate	▪ Middle management control responsibility must be specified.	▪ Half yearly periodic review and monitoring.
4.	High / High High	▪ Senior management attention and action needed.	▪ Quarterly periodic review and monitoring.
5.	Extreme	▪ Requires detailed research, planning and decision making at Board of Director level.	▪ Immediate action with monthly review and monitoring for the 1st year.

APPENDIX 7 : CONTROLS EFFECTIVENESS RATINGS DEFINITION

Control Effectiveness Rating	Description
Very Good	All controls are in place and well implemented
Good	Sufficient controls are in place
Satisfactory	Controls require additional improvements
Some Weakness	Insufficient controls. Improvement critically required
Weak	Controls fail

APPENDIX 8 : RISK RATING DEFINITION

Gross Risk Rating	Residual Risk Rating	Target Risk Rating
Risk rating based on the approved risk criteria /appetite (likelihood and consequences) **before** the consideration of effectiveness of existing controls	Risk rating based on the approved risk criteria/appetite **after** that consideration of effectiveness of existing controls	Desired / intended risk based on the approved risk criteria/appetite considering mitigating strategies that can still be determined and implemented for certain period of time.

APPENDIX 9: AWARDS & ACHIEVEMENT

ASEAN RISK AWARD 2021

WINNER
ASEAN RISK CHAMPION (CATEGORY 2)

This award is presented to the organization that has proven itself to be able to lead ground-breaking Risk Management approach that tackles the challenges and exploit opportunities in today's world

RUNNER UP
RISK INNOVATION

As innovation leads us to a better world, this award is presented to the organization that have contributed to the advancement of Risk Management knowledge and practice by finding new ways in its implementation