AME ELITE CONSORTIUM BERHAD

Registration No. 201801030789 (1292815-W)
(Incorporated in Malaysia)

RISK MANAGEMENT FRAMEWORK

KEY TERMS

Inherent Risk
The level of impact and likelihood of risk before any control or risk mitigation is applied.

Residual Risk
The remaining risk(s) after controls has been put in place.

Risk(s)
Risk is anything that has the potential to prevent the Group from achieving its overall goals and objectives.

Risk Appetite
Risk appetite is defined as the level of risk the Group is prepared to accept to achieve its objectives measurable in terms of the variance of return (i.e. risk) to accomplish a desired result (i.e return) as set out in the risk parameters.

Risk Impact/Consequence
An evaluation of the significance of a particular risk to the Group. The magnitude of impact is determined in relation to the organisation's risk appetite and organisational objectives.

Risk Management
Risk management is a continuous, proactive and systematic process to recognise, manage and communicate risk from an organisation-wide perspective. It is all about making strategic decisions that achieve the Group's overall corporate objectives.

Risk Owner
Individual with overall responsibility for managing an identified risk.

Risk Parameter
Used to estimate the impact of a risk should it occur and will be based on the Group's risk appetite.

1. INTRODUCTION

This Risk Management Framework ("**Framework**") is to provide a structured and proactive approach towards managing risks for AME Elite Consortium Berhad ("**AME**" or "**Company**") and its subsidiaries (collectively referred to as the "**Group**").

It covers risk management policies designed to achieve the Group's strategic objectives and lists out risk management processes necessary to implement and monitor compliance with the policies. This Framework also outlines the roles and responsibilities of the Board of Directors of AME ("**Board**"), the Audit and Risk Management Committee of AME ("**ARMC**"), the Risk Management Working Group ("**RMWG**") and other employees within the Group to ensure all directors and employees within the Group are aware of their roles, duties and responsibilities in the context of risk management.

The standards and policies of this Framework are founded on the principles and guidelines of *ISO 31000 Risk Management*.

2. OBJECTIVES

The primary objectives of this Framework are as follows:

a) to support the overall achievement of the Group's strategic objectives;
b) to create a risk-attuned environment to safeguard the Group's resources, people, finance, property and reputation;
c) to provide a structured and consistent approach to identifying, rating, mitigating, managing and monitoring risk;
d) to outline the risk context of the Group, which comprises its values, strategies, policies and operating system to better manage the business, project or any risk exposures confronted by the Group;
e) to provide guiding risk management principles to the respective Heads of Department/Division ("**HOD**") to assist them in governing the actions of their individual personnel concerning managing risks; and
f) to provide feedback and assure the management that there is an appropriate framework and internal control to identify, analyse, evaluate, manage and monitor significant financial and non-financial risks.

3. APPLICABILITY

This Framework covers all activities, processes, projects, products, services, assets and systems currently in the Group. It applies to all directors, management and employees (including full-time, probationary, contract and temporary staff) of the Group.

Each Director or Employee must read and understand the Framework. Any person who requires further clarification on the Framework may refer to the Chief Risk Officer ("**CRO**") or the Chief Financial Officer of AME.

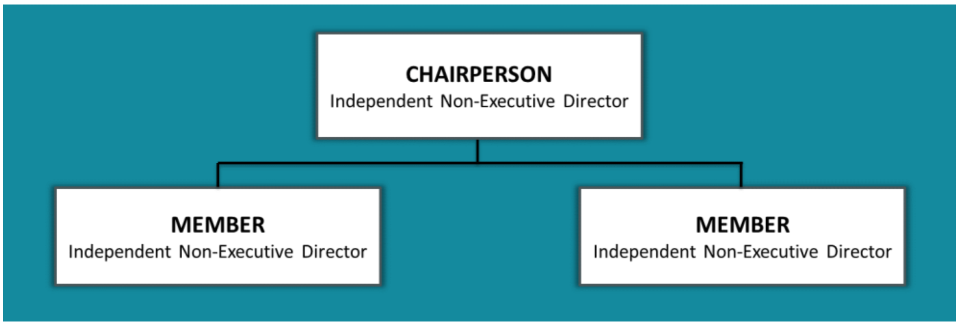
4. STRUCTURE AND COMPOSITION

4.1 Risk Organisation Structure

As illustrated below, the risk organisation structure of AME is established for effective risk management.

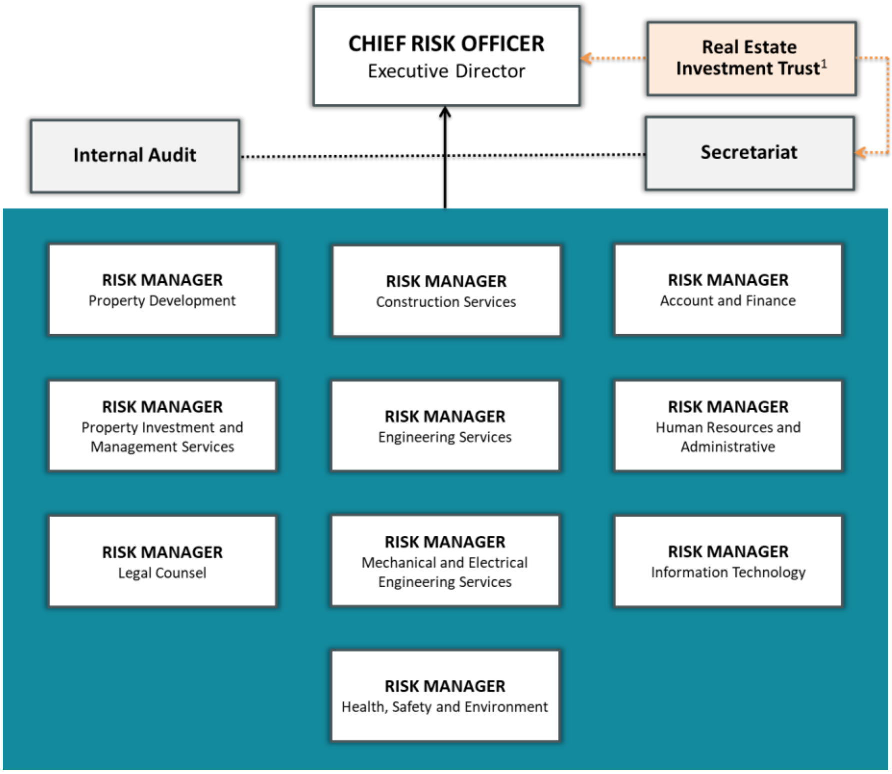
4.2 Audit and Risk Management Committee Structure

The Audit and Risk Management Committee of AME comprise solely of Independent Directors.



4.3 Risk Management Working Group Structure

The RMWG of AME oversees and coordinates the Group's risk management at the respective Divisions and/or Departments.



[1] For AME Real Estate Investment Trust ("**AME REIT**"), an indirect 51% owned entity of AME which was listed on the Main Market of Bursa Malaysia Securities Berhad on 20 September 2022, the risk management is carried out by I REIT Managers Sdn Bhd ("**IRM**"), the management company of AME REIT and a wholly owned subsidiary of AME. As for IRM, the risk management shall be delegated to the Board of IRM, its ARMC and/or their delegates.

For both AME REIT and IRM, any significant risk management matter shall be reported to the CRO of AME.

5. ROLES AND RESPONSIBILITIES

5.1 Board of Directors

The Board of Directors of AME is ultimately responsible for the overall risk management monitoring. It should provide guidance and instructions on risk management matters and ensure the implementation of appropriate systems and/or guidelines to manage risks confronted by the Group.

In tandem with the Company's Board Charter, the roles and responsibilities of the Board in risk management include, but are not limited to, the following:

a) Ensure there is a sound framework for risk management and internal control;
b) Understand the principal risks of the Group's business and recognise that business decisions involve the taking of appropriate risks; and
c) Set the risk appetite within which the Board expects management to operate and ensure an appropriate risk management framework to identify, analyse, evaluate, manage and monitor significant financial and non-financial risks.

5.2 Audit and Risk Management Committee

The Audit and Risk Management Committee of AME oversees the Group's risk management framework and policies.

The roles and responsibilities of the ARMC in risk management include, but are not limited to, the following:

a) Review and recommend risk management policies and procedures for the Board's approval;
b) Assess the adequacy and effectiveness of the risk management processes; and
c) Review the risk profile of the Group (including risk registers) and the risk management team's plans to mitigate business risks as identified from time to time.

5.3 Risk Management Working Group

The RMWG of AME is established at the Group level, which comprises members from major subsidiaries of the Group and/or functional divisions/departments. The core role of the RMWG is to implement risk management policies adopted by the Board with recommendations by the ARMC.

The roles and responsibilities of the RMWG include, but are not limited to, the following:

a) Identify and evaluate the risks faced by the Group for consideration by the Board with recommendations by the ARMC; and

b) Review and update the Group's risk management methodologies applied, specifically those related to risk identification, measuring, controlling, monitoring and reporting.

5.4 Chief Risk Officer

The CRO of AME, who leads and guides the RMWG, is primarily accountable for the effectiveness of the Group's risk management system.

The roles and responsibilities of the CRO include, but are not limited to, the following:

a) Lead and guide the RMWG;
b) Serve as the central contact for risk management issues within the Group;
c) Coordinate risk management routinely within the Group;
d) Supervise risk management policy implementation at the Group level;
e) Report the Group's risk profile (which is generated by the Company's major subsidiaries) to the Board and the ARMC yearly;
f) Participate in business planning activities to allow for consideration of risks in business plans and budgets; and
g) Monitor the progress of risk action plans and liaise with the respective Risk Managers on the action plans.

5.5 Secretariat

The Secretariat in risk management of AME is responsible for coordinating risk management at Group level. The Secretariat will centrally manage any update to the Group's risk register and other guidelines.

The roles and responsibilities of the Secretariat in risk management include, but are not limited to, the following:

a) Assist both the ARMC and the CRO in their administrative activities;
b) Maintain the Group's risk register;
c) Coordinate and compile the Group's risk profile generated by major subsidiaries for the Board's discussion;
d) Communicate policies established to the respective Risk Managers at the department/division level; and
e) Assist in monitoring the progress of risk action plans and liaising with respective Risk Owners on the action plans.

5.6 Risk Managers

The Risk Managers are the HOD who are directly responsible for the day-to-day operation of their respective departments/divisions.

The roles and responsibilities of the Risk Managers include, but are not limited to, the following:

a) Accept the risk owner concept to own and manage their risks;
b) Promote risk awareness by introducing risk management objectives within their operations;
c) Ensure risk management is a regular agenda in their department/division meeting to allow consideration of exposures and to reprioritise work in light of effective risk analysis;
d) Manage risks on a day-to-day basis by identifying risks and managing risks based on the risk management policies contained herein;
e) Apply the principles and processes of risk management at the conceptual stage of projects as well as throughout the project's lifecycle; and
f) Update the risk registers within their area of responsibility for the Board and the ARMC's consideration.

5.7 Internal Audit Function

The primary role of the internal audit function concerning risk management is to assure the Board on the effectiveness of risk management.

The roles and responsibilities of the Internal Audit function include, but are not limited to, the following:

a) Periodically audit the Group's risk management practices and provide recommendations on improvement to management and the ARMC;
b) Ensure the adequacy of risk management policies;
c) Examine and evaluate the appropriateness and effectiveness of risk management processes; and
d) Evaluate the reliability (including integrity, accuracy and comprehensiveness) and timeliness of risk management information.

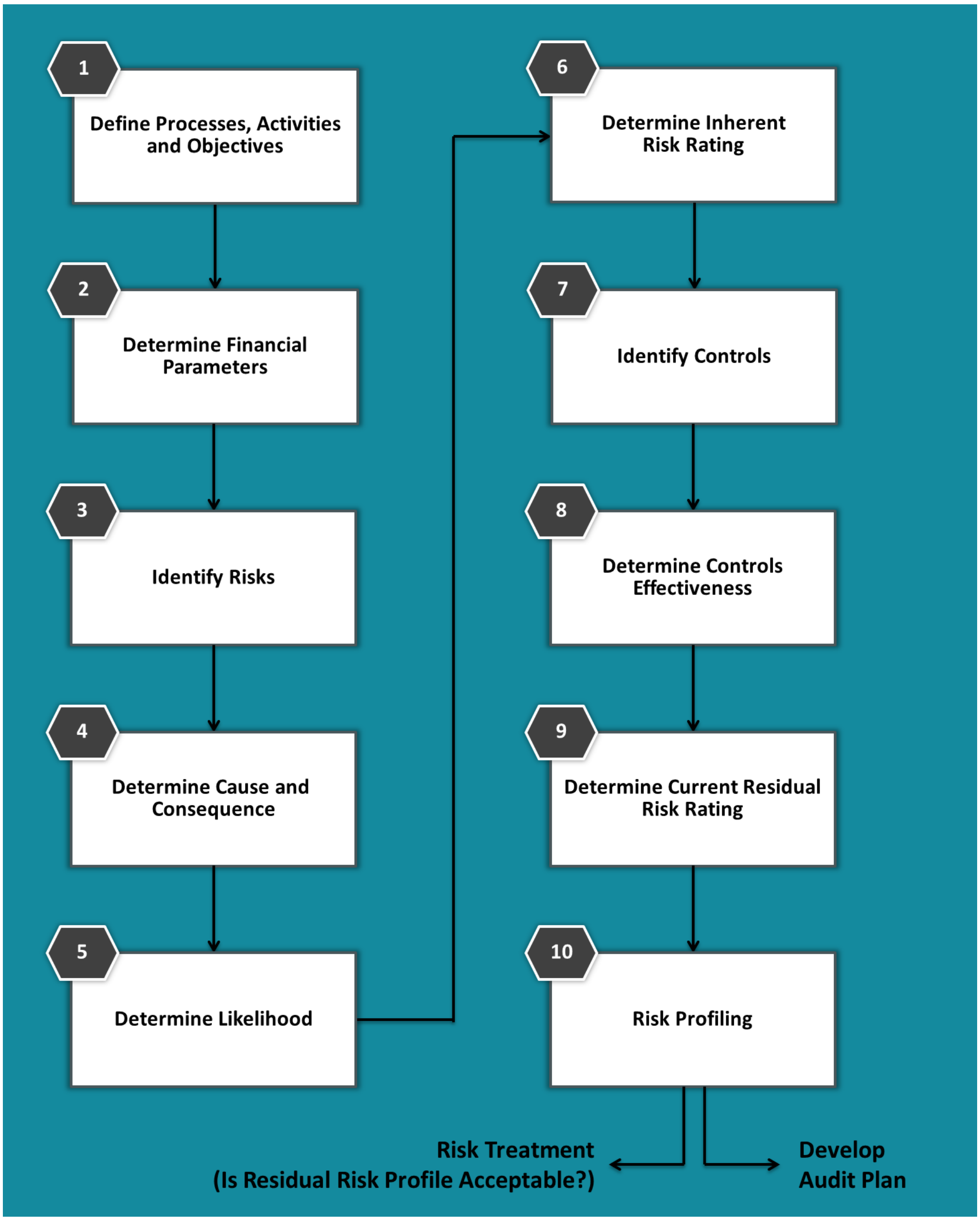
5.8 All Employees within the Group

All employees within the Group shall have a general duty of care and are responsible for complying with requests from management in connection with the application of this Framework.

Employees must be conscious of the risks related to their actions and decisions. All reasonable care should be taken through appropriate preventive actions to prevent the loss, maximise opportunity and ensure that the Group's operations, reputation and assets are not jeopardised.

6. RISK MANAGEMENT PROCESS

The diagram below provides an overview of the Group's risk management process.



Step 1: Define Processes, Activities and Objectives

To ensure all the key risks have been raised and identified, the first step of the risk management process is to define the key processes, activities and objectives of the respective departments/divisions. The information is then used as a guide or "map" in the subsequent steps.

Example:	
Process:	**Activities:**
Human Resource Management	• Recruitment • Training • Performance Appraisal • Counselling

Step 2: Determine Financial Parameters

Financial loss is the key measure used to describe the consequence of a risk event occurring. It can be measured using a value (e.g. profit before tax), or it could be a physical measure (e.g. the number of days delay in project progress). The financial parameters are categorised according to the impact on the operational unit being examined.

The financial parameters will be based on the Group's risk appetite, which is defined as the level of risk the Group is prepared to accept to achieve its objectives. The risk appetite of the Group can be expressed in terms of how much variability of return (i.e. risk) the Group is prepared to accept to achieve a desired level of result (i.e. return). This exercise aims to determine how much risk the Group is willing to undertake.

Further, reference will be made to the Group's risk capacity, which is defined as the level of risk the Company is not prepared to exceed. In other words, the risk capacity represents the maximum loss the Group can sustain in any year before the Group would face going concern problems.

The risk appetite of the Group is generally defined as follows:

RISK RATING	DESCRIPTION	MIN. ACTION REQUIRED
Very High Risk	Immediate action is required in consultation with management to avoid the risk entirely or to reduce the risk to a tolerable, low or very low rating.	Avoid and/or Mitigate
High Risk	These risks need to be mitigated with actions as required, and managers need to be assigned these risks.	Accept and/or Mitigate
Tolerable	Managed by specific monitoring or response procedures.	Accept and/or Mitigate
Low Risk	Managed by routine procedures.	Accept
Very Low	Managed by routine procedures.	Accept

Step 3: Identify Risks

Risk identification determines *what, where, when, why,* and *how* events could prevent, degrade, delay or enhance the achievement of the Group's objectives.

Identifying key risks to the Group is a critical step in effective risk management and needs to be comprehensive. If a potential risk is not identified timely and is omitted from further analysis, a material risk may be given insufficient attention. Identification should include all risks, whether or not they are under the control of the Group.

The following questions can be used to assist in identifying risks:

Questions:	
How could we fail?	What must go right for us to succeed?
Where are we vulnerable?	What assets do we need to protect?
How could someone steal from the Company?	How could someone disrupt our operations?
On what do we spend the most money?	What activities are the most complex?
What decisions require the most judgment?	On what information do we most rely on?
How do we bill and collect our revenue?	How do we know whether we are achieving our objectives?

Step 4: Determine Cause and Consequence

The next step is to identify the possible causes and consequences of each risk identified. A single risk event may have specific or multiple possible causes or effects. However, a single cause or effect may apply to multiple risks.

The main causes of the risk will be used to determine which broad risk category the risk should be recorded, whereas a rating is assigned to each risk based on the consequences described.

Example:	
Cause:	**Consequence:**
One of the risks identified may be: **Loss of key personnel** **Causes** may include: • uncompetitive remuneration; • poaching by competitors; • poor training and development; • poor working conditions; and/ or • perceived lack of career opportunities. After reviewing the main causes, the risk would be included in the **Human Resources** broad risk category.	Effects may be identified as flowing from the risk of losing **key personnel**. **Effects** may include: • recruitment costs; • production interruption; • training costs; • loss of morale; and/ or • reputation damage. After reviewing the possible effects the risk would be rated as a **Moderate** consequence.

The effect ratings of the Group are as follow:

EFFECT RATING	DESCRIPTION
Catastrophic	Extraordinary event with the potential to lead to collapse.
Major	A critical event which requires exceptional management effort.
Moderate	A serious event which requires additional management effort.
Minor	An adverse event which can be absorbed with some management effort.
Insignificant	Impact can be readily absorbed through normal activity.

Step 5: Determine Likelihood

This likelihood assessment step requires the assignment of a likelihood rating to each identified risk. Consideration should be given to:

- the anticipated frequency of the event occurring;
- the working environment;
- the procedures and skills currently in place;
- staff commitment, morale and attitude; and
- history of previous events.

The likelihood ratings of the Group are as follows:

LIKELIHOOD RATING	DESCRIPTION	LIKELIHOOD
Almost Certain	The risk is almost certain to occur more than once within the next 12 months unless controlled (high likelihood of occurrence unless controlled).	More than 90%
Likely	The risk is almost certain to occur at least once within the next 12 months unless controlled.	More than 50% to 90%
Moderate	The risk could occur at least once in the next 1 to 3 years (some likelihood of risk occurring unless controlled).	More than 25% to 50%
Unlikely	The risk could occur at least once in the next 3 to 5 years.	More than 5% to 25%
Rare	The risk is unlikely to occur in the next 5 to 10 years (very low potential for occurrence).	Less than 5%

Step 6: Determine Inherent Risk Rating

The consequence and likelihood ratings identified above are used to determine the inherent risk rating for each risk in a risk assessment matrix. It involves mapping the parameters for the magnitude of the impact of a risk against the likelihood parameters.

There should be only one overall inherent risk rating for each risk, regardless of whether multiple causes or consequences have been identified.

The risk assessment matrix of the Group is as follows:

CONSEQUENCE	Rare	Unlikely	Moderate	Likely	Almost Certain
Catastrophic	Tolerable	High	Very High	Very High	Very High
Major	Low	Tolerable	High	Very High	Very High
Moderate	Low	Low	Tolerable	High	High
Minor	Very Low	Low	Tolerable	Tolerable	High
Insignificant	Very Low	Very Low	Low	Tolerable	Tolerable

LIKELIHOOD

Step 7: Identify Controls

Controls identification is to determine and describe whether any existing control is in place that either reduces the likelihood of an event occurring or reduces the potential consequence arising from the event. For each risk identified, there may be a single or multiple controls to address the risk. If there is no existing control, there is a control gap.

Further, the owner of the control identified has to be determined in this step. The controlling owner is the person or role with accountability for ensuring that the control activity is in place and operating effectively. The controlling owner does not necessarily perform the control activity. However, they should have a level of oversight of their performance.

Example:

Identified Risk: **Loss of key personnel**

Existing Controls

- awareness of market remuneration levels;
- regular remuneration reviews;
- well-developed training program;

Additional Controls

- to implement succession planning
- to establish career development program

Control Owner: **Head of Human Resources Department**

Step 8: Determine Controls Effectiveness

Once the key controls have been identified, assessments are to be made to determine the overall effectiveness of the controls in terms of the strength of their design and operations. Results of such assessments will be presented by assigning a control rating to the relevant controls.

The control ratings of the Group are as follows:

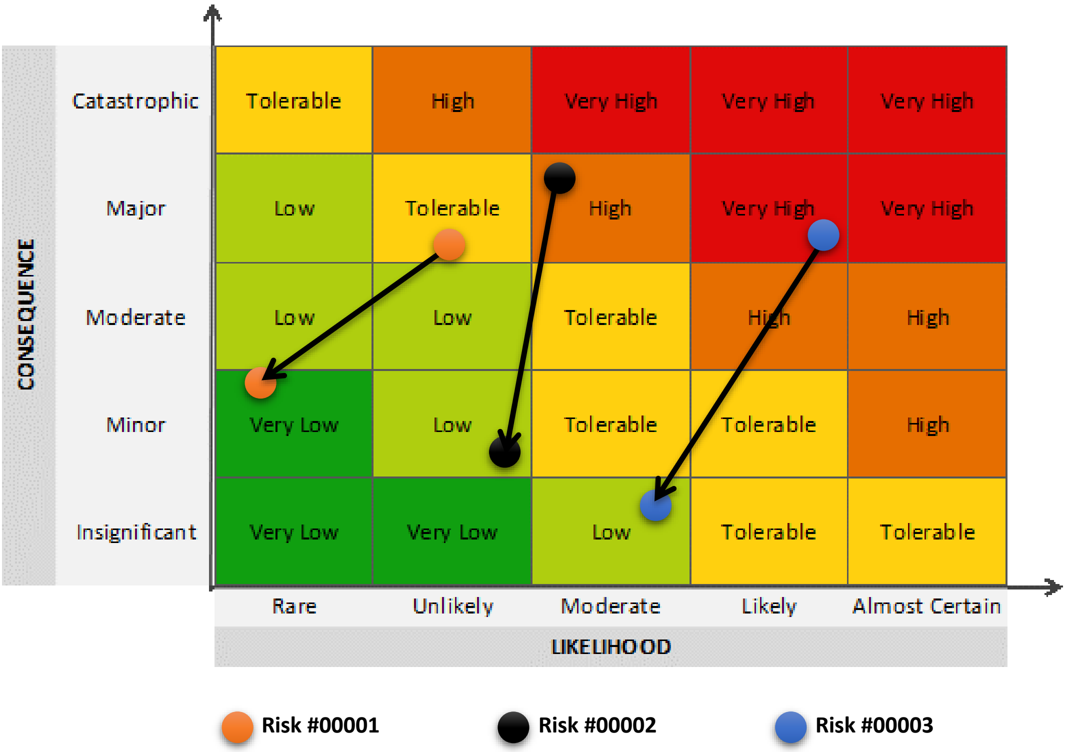
CONTROL RATING	DESCRIPTION
None	Controls and/or management activities are non-existent or have major deficiencies and don't operate as intended.
Needs Improvement	Limited controls and/or management activities are in place, high level of risk remains.
Adequate	Controls and/or management activities are in place, with opportunities for improvement identified.
Strong	Controls and/or management activities are properly designed and operating, with limited opportunities for improvement identified.
Effective	Controls and/or management activities are properly designed and operating as intended.

Step 9: Determine Current Residual Risk Rating

The residual risk represents the risk, which remains after considering the controls in place to mitigate the risk.

This rating combines the inherent risk rating (Step 6) and the control effectiveness rating (Steps 7 and 8). For example, if the controls were "Effective", the inherent risks categorised as "Very High" would be moved down towards the "Low" or "Very Low" areas of the matrix.

The residual risk matrix below illustrates the movement of the inherent risk to residual risk after considering the control effectiveness in place, which mitigates the inherent risks mentioned in step 6.



Step 10: Risk Profiling

Once the risk registers and residual risk ratings are confirmed, a risk profile shall be prepared.

After this risk assessment process, the management must consider the residual risk levels and decide whether they are acceptable in the context of the Group's objectives. The objective is not to eliminate all residual risks but rather to ensure that any residual risk is maintained at an acceptable level cost-effectively.

7. RISK TREATMENT

Risk treatment involves developing a range of options for mitigating the risk, assessing those options, and then preparing and implementing action plans. The highest rated risks should be addressed as a matter of urgency.

Selecting the most appropriate risk treatment means balancing the costs of implementing each activity against the benefits derived. The cost of managing the risks needs to be commensurate with the benefits obtained. When making cost versus benefit judgements the wider context should also be considered The risk profile of the Group enables the management to make conscious and visible risk management decisions. Depending on the type and nature of the risk, the following options are available:

TREATMENT	DESCRIPTION
Avoid	Avoiding the risk by deciding not to proceed or continue with the activity that gives rise to the risk or by seeking an alternative means to achieve the objective.
Reduce	Reducing the risk by the application of controls or management action plans. The controls or action plans may be by removing the risk source, changing the likelihood and/or changing the impacts. *(It may not be possible to eliminate risks entirely and some net risk may still remain)*
Share or Transfer	Sharing the risk with another party or parties e.g. through a contractual arrangement and risk financing.
Accept	Taking or increasing risk to pursue an opportunity and be prepared to manage its consequences/impacts. *(As a general rule, such risks are those that will lead to relatively small losses, however such risks, if commonly occurring should be monitored cumulatively)*

8. RISK MONITOR AND REVIEW

Monitoring and review should be a planned part of the risk management process and involve regular checking or surveillance. The results should be recorded and reported externally and internally, as appropriate. The results should also be an input to the review and continuous improvement of the Group's risk management framework.

9. REVIEW OF THE FRAMEWORK

This Framework shall be reviewed by the Board at least once every three (3) years or as required when internal or external events warrant a more frequent review to be undertaken.

The Board adopted this Framework on 26 February 2020. The Board reviewed it on 24 February 2023.