# PRESTARIANG BERHAD

# RISK MANAGEMENT FRAMEWORK

2012

## EXPLANATORY FOREWORD

Companies face risks from many sources and virtually, all areas of the business are exposed to risks. Therefore, it is imperative that Companies are able to assess and manage their risks and that their stakeholders are informed of the risk management policies and practices. Moreover, in practicing good corporate governance, Companies are encouraged to disclose, inter-alia, their risk management policies in line with the efforts of certain authorities to enhance transparency in a disclosure-based regime.

In line with the above, the main objectives of this Risk Management Framework (Framework) are to provide guidance to the management of Prestariang Berhad to facilitate a structured framework approach to risk management and to achieve a level of adequate and standard risk reporting.

Broadly, the Framework deals with: -

- The corporate risk management policy;
- The roles of the Board of Directors, the Audit Committee, the Management, the Risk Management Committee; and
- The Risk Management process.

Except where the context otherwise requires, the following definitions shall apply throughout the framework: -

| | | |
|---|---|---|
| Prestariang or the Company | - | Prestariang Berhad |
| Prestariang Group or the Group | - | Prestariang Berhad and its major operating subsidiaries & associates |
| Subsidiaries or Associates | - | Major Operating Subsidiaries and Associates of Prestariang Berhad |
| Board of Directors or BOD | - | Members of the Board of Directors of Prestariang Berhad |
| Audit Committee or AC | - | Members of the Audit Committee of Prestariang Berhad |
| RMC | - | Risk Management Committee |

## CONTENTS

# SECTION I: CORPORATE RISK MANAGEMENT POLICY

## 1. WHAT IS RISK MANAGEMENT?

It is inevitable that risks will always exist in an organisation and these risks should be managed or controlled. Risk control does not, and should not, mean risk avoidance. It means measuring and controlling exposures and knowing the limits that are acceptable to the organisation.

Risk is the chance of something happening that will have an impact upon objectives. It is measured in terms of likelihood and consequences[1]. Risk arises as much from the possibility that opportunities will not be realised as it does from the possibility that threats will materialise.

Managing risk is about reacting to the changes within the organisation as well as the organisation's response to changes in the environment. Managing risk is a shared responsibility and therefore, the management of risk should be integrated into the managerial framework of an organisation. It is an iterative process consisting of steps which, when undertaken in sequence, enable continual improvement in decision-making.

The risk management process is a logical and systematic method of identifying, analysing, assessing, treating, monitoring and communicating risks with any activity, function or process in a way that will enable an organisation to minimise losses and maximise opportunities. It should be noted that:

- Risks, particularly inherent risks, cannot be eliminated in their entirety;
- Risks must be evaluated in terms of likelihood of an event occurring and not merely in terms of impact; and
- The management of risk should somehow try to equate the benefit of risk reduction with the cost of risk reduction.

The risk management process works on the basis of developing a corporate wide Consolidated Risk Profile for the Prestariang Group. Within Prestariang this will then be filtered down to the respective Companies, Divisions and appropriate projects; which will in turn create their own risk registers. On a group wide basis the "**significant**" and "**high**" risks at subsidiary & associate level will be filtered up into the Prestariang consolidated risk register where applicable.

[1] AS/NZS 4360:2004 Risk Management Standard

## 2. POLICY AND OBJECTIVES

The Prestariang risk management process is based on the following policy and designed to achieve the following key objectives: -

### 2.1 Risk Management Policy

Generally, the risk management policy of Prestariang aims to put in place adequate and effective risk management processes to manage risks to achieve business objectives and provide reasonable assurance to the Board of Directors and other stakeholders on the state of risk management as part of system of internal controls of the Company and its ability to increase shareholders' value and confidence.

### 2.2 Key Objectives

The key objectives for risk management are: -

2.2.1 To enhance the decision making process within Prestariang in order to: -

a. Fulfil the Company's strategic objectives;

b. Optimise the return to shareholders taking into account the interests of other stakeholders; To ensure appropriate and timely responses to changes in the environment that affect the Company's ability to achieve its objectives;

2.2.2 To improve the Company's operating performance;

2.2.3 To reduce risks of material misstatement in official announcements and financial statements;

2.2.4 To create a risk attuned environment to safeguard the Company's assets (property and investments) and maintain its reputation; and

2.2.5 To fully comply with the Malaysian Code of Corporate Governance, the relevant laws including the Listing Requirements of Bursa Malaysia (where applicable).

### 2.3 Management Guiding Principles

Prestariang has the following risk management guiding principles to achieve the aforementioned policy and objectives: -

2.3.1 Strategic and Operations

a. Ensuring an effective quality management system is in place.

b. Implementing an effective internal control framework, which is reviewed periodically by the management team.

c. Complying with the Limits of Authority (LOA), policies and procedures of the Company at all times.

d. Complying with all regulations, legislation and by-laws.

e. Adequately insuring and maintaining key assets of the Company.

2.3.2 Information System

a. Implementing and ensuring an effective and efficient information security system which must be continuously monitored.

b. Ensuring continuous availability of the system to support business operations and decision-making.

2.3.3 Financial and Accounting

a. Adopting prudent and sound accounting and financial policies with appropriate approval channels.

b. Maintaining accurate, reliable and current financial information.

c. Ensuring compliance with relevant Financial Reporting Standards (FRS).

2.3.4 Human Resource

a. Having in place a competent and adequately staffed workforce.

b. Having in place a succession program for all key management personnel.

## 3. RISK APPETITE

In determining whether a risk is acceptable to the Company, the Board of Directors with recommendation by the Audit Committee and the Risk Management Committee must firstly ascertain the risk appetite of the Company.

Risk appetite refers to the risk tolerance vis-à-vis the returns, or simply the extent of risk that a company can take or tolerate in relation to the potential gains or advantage for a specified condition.

In computing the risk appetite of Prestariang, the relevant industry risk appetites e.g. the expected return on investment ("ROI"), return on capital employed ("ROCE"), the internal rate of return ("IRR"), **or any other means, can be taken into consideration**.

Because risk management is an ongoing process, the risks to which Prestariang is subject to, and stakeholders' tolerances for these risks, will evolve. Therefore, the risk appetite may change over time in line with changes.

## 4.1 Unacceptable Risk

The following are the risks that are considered unacceptable to Prestariang. This list should be adapted as relevant and/or expanded to comprehensively address the significant risks of the Company taking into consideration changes in various factors such as, risk appetite; the economic environment; and etc. Amendments should be approved by the Board of Directors with recommendation by the Audit Committee.

| Unacceptable risk | |
|---|---|
| 4.1.1 | **Non-compliance** with: -<br>• Federal, state and local legislation, regulation and by-laws, which could have an adverse impact on the reputation and going-concern status of the company.<br>• Covenants and obligations resulting in triggering default, suspension or de-listing (where applicable). |
| 4.1.2 | Risks that **impact** negatively on: -<br>• The going concern status of the Company.<br>• Solvency.<br>• Security and safety concerns of the business/projects, which can result in prolonged cessation of business arising from, stop work orders or other actions taken against the Company. |
| 4.1.3 | Risks of accepting projects where there may be: -<br>• Failure to **deliver**[2] on time (including extension of time), within specification or required performance, which result in termination of project or negative reputation to the Company.<br>• Failure to keep within budget (**5% negative impact**). |
| 4.1.4 | Risks that result in: -<br>• Prolonged suspension or de-listing (where applicable) from the Bursa Malaysia (Bursa).<br>• Classification as a PN17 company (where applicable).<br>• Downgrading of debt instrument ratings to non-investment grade level. |
| 4.1.5 | Loss of critical data or **information** resulting in business interruptions or business opportunities foregone or usage of information for unauthorised purposes. |
| 4.1.6 | Risks that **impact negatively** on relationship, resulting in: -<br>• Severance of goodwill or ties with Government, authorities and stakeholders.<br>• Loss of major customer (**5% or more of Group revenue**). |
| 4.1.7 | Risks involving **staff** that impact negatively on the company in connection with: -<br>• Industrial disharmony that damages the reputation of the company and/or affects operations.<br>• Inadequate health and safety standards resulting in detrimental image and/or affect ongoing operations.<br>• Lack of succession and continuity of key positions.<br>• Employees who have committed fraud or have been convicted of criminal offences.<br>• Employees who are proven to be incompetent or negligent or have breached their duty as an employee. |

[2] Based on benchmark or judgment of operating companies/division

## 5.1 Statement of Acceptable Risk

In determining the acceptable risks to Prestariang, financial and non-financial factors need to be taken into consideration. In general the various degrees of acceptable risks are guided by the Profit Before Tax (PBT) and Shareholders Fund (SHF) for the relevant financial period.

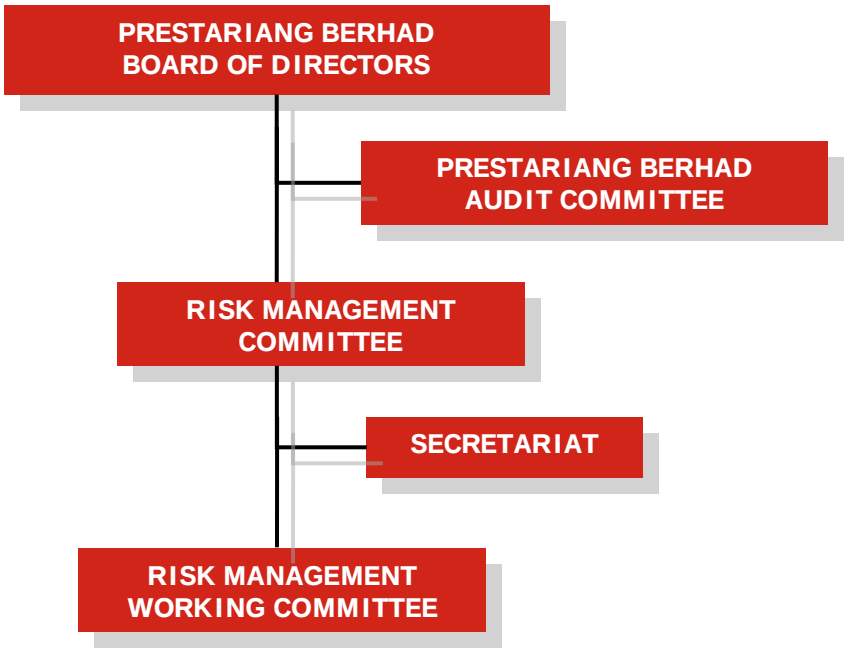
| Category | Guidelines (whichever is lower)PBT OR SHF |
|---|---|
| Acceptable (Managed by routine procedures) | • Insignificant financial implication.<br>• No potential impact on market share.<br>• No impact to the Company's reputation and/or operations. |
| Acceptable subject to **monitoring on cumulative impact** (Managed at departmental level) | • Up to **1%** adverse impact on consolidated PBT[3] **OR**<br>• Up to **0.10 %** adverse impact on shareholders funds.<br>• Consequences that can be absorbed under normal operating conditions.<br>• Potential impact on market share or reputation of the Company. |
| Acceptable subject to **risk treatment** and/or close monitoring (Can be left to operating management) | • Above **1%**, up to **5%** adverse impact on consolidated PBT **OR**<br>• Above **0.10%** up to **0.25%** adverse impact on shareholders funds.<br>• Market share, reputation or value of Company will be affected in the short-term. |
| Acceptable subject to **extensive risk treatmen**t and/or close monitoring (Need Senior/Top Management Attention) | • Above **5%**, up to **15%** adverse impact on consolidated PBT **OR**<br>• Above **0.25%** up to **1%** adverse impact on shareholders funds.<br>• Key alliances are threatened.<br>• Market share, reputation or value of Company will be affected in the short-term. |
| Only acceptable if **prior approval** is obtained from the Board and subject to close monitoring and frequent updates to the Board | • More than **15%** adverse impact on consolidated PBT **OR**<br>• More than **1%** adverse impact on shareholders funds.<br>• Risk outweighs returns.<br>• Serious diminution in market share, reputation or value of Company with adverse publicity. |

[3] Profit refers to the budgeted or planned profit before taxation for the relevant period

# SECTION II: ROLES OF THE BOARD OF DIRECTORS, THE AUDIT COMMITTEE, THE MANAGEMENT AND THE RISK MANAGEMENT COMMITTEE

## 1. STRUCTURE AND COMPOSITION

### 1.1 Structure




### 1.2 Composition

1.2.1 The Risk Management Committee (RMC) of Prestariang consists of the following Independent Non-Executive Directors:

a. Ramanathan A/L Sathiamutty as the Chairman of the RMC;
b. Paul W Chan; and
c. Dr Abu Hasan Ismail

1.2.2 Co-opted members from the Management team making up the Risk Management Committee in the working group headed by the Risk Manager as and when needed:

a. Chief Executive Officer;
b. Chief Operating Officer;
c. Chief Financial Officer; and
d. Representatives from subsidiaries (as and when required).

## 2. THE ROLE OF THE BOARD OF DIRECTORS

The Board of Directors sanctions the objectives and the risk management policy expressed in this Framework.

The stewardship responsibilities of the Board of Directors[4] include: -

a. Identifying and acknowledging principal risks as identified by the RMC and ensuring the implementation of appropriate systems to manage these risks;

b. Reviewing the adequacy and the integrity of the Company's system of internal controls and management information systems, including systems for compliance with applicable laws, regulations, rules, directives and guidelines.

Principle D II in Part I of the Malaysian Code on Corporate Governance 2000, which reads - *"The Board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets"*, clearly places the onus for internal control on the Board of Directors.

Further to the above, the Board should also consider the following: -

a. The nature and extent of downside risks acceptable for Prestariang to bear within its particular business;

b. The risk implications of Board decisions.

To help meet its responsibilities in relation to internal control, the Board should set appropriate policies on internal control and seek regular assurance that will enable it to satisfy itself that the system is functioning adequately and that its integrity is maintained. The Board must further ensure that the internal controls are adequate in managing the risks of the Company.

[4] Part AA Section 1 of the Code of Corporate Governance

## 3. THE ROLE OF THE AUDIT COMMITTEE

The following is the main duties and responsibilities of the Audit Committee: -

a. Assist the Board of Directors in identifying the principle risks in the achievement of the Company's objectives and ensuring the implementation of appropriate systems to manage these risks.

## 4. THE ROLE OF THE RISK MANAGEMENT COMMITTEE AT PRESTARIANG LEVEL

The functions of the RMC include: -

a. Reviewing and recommending the risk management policies and procedures for the approval or acknowledgement of the Board with recommendation by the Audit Committee.

b. Acting as Primary Champion of risk management at strategic and operational levels.

c. Reviewing the on-going adequacy and effectiveness of the risk management process.

d. Undertaking reviews of the consolidated risk register of major subsidiaries and associates within the Group to identify significant risks and whether these are adequately managed.

e. Ensuring that the Board and Audit Committee receive adequate and appropriate information (including the annual Risk Report) for decision-making and review respectively.

f. Commissioning, where required, special projects to investigate, develop or report on specific aspects of the risk management processes of the Company.

The RMC meets at least **every quarterly**.

## 5. THE ROLE OF THE SECRETARIAT

The role of the Secretariat is as follows: -

a. Assisting the RMC in its administrative activities.

b. Coordinating and compiling the risk profiles generated by major subsidiaries and associates for the purpose of deliberation at Prestariang level.

c. Maintaining the risk register of Prestariang.

d. Communicating policies and limits established by the RMC to the respective risk management committees at subsidiary and associate level.

e. Liaison between the RMC and the respective Risk Owners.

f. Follow-up on Board approved risk action plans for the purpose of reporting to the RMC.

## 6. THE ROLE OF THE RISK MANAGEMENT WORKING COMMITTEE

It is the role of the Management Working Committee to implement Board policies on risk and control. In fulfilling its responsibilities the Management Working Committee of Prestariang: -

a. Identifies and evaluates the risks faced by Prestariang for consideration by the Board with recommendation by the Audit Committee and RMC.

b. Ensures that risk management working committee is a regular agenda/item in their management meetings to allow consideration of exposures and to reprioritise work in light of effective risk analysis.

c. Ensures that risk management working committee is incorporated at the conceptual stage of projects as well as throughout the project's lifetime.

d. Implements policies adopted by the Board with recommendation by the Audit Committee through a suitable risk management framework.

## 7. THE ROLE OF THE RISK OWNERS

The roles of the Risk Owners are: -

a. Promoting risk awareness by introducing risk management objectives within their operations.

b. Ensures that risk management is a regular agenda/item in their departmental/divisional meetings to allow consideration of exposures and to reprioritise work in light of effective risk analysis.

c. Managing risk on a day-to-day basis by identifying risk and managing risk based on the policies of risk management contained herein.

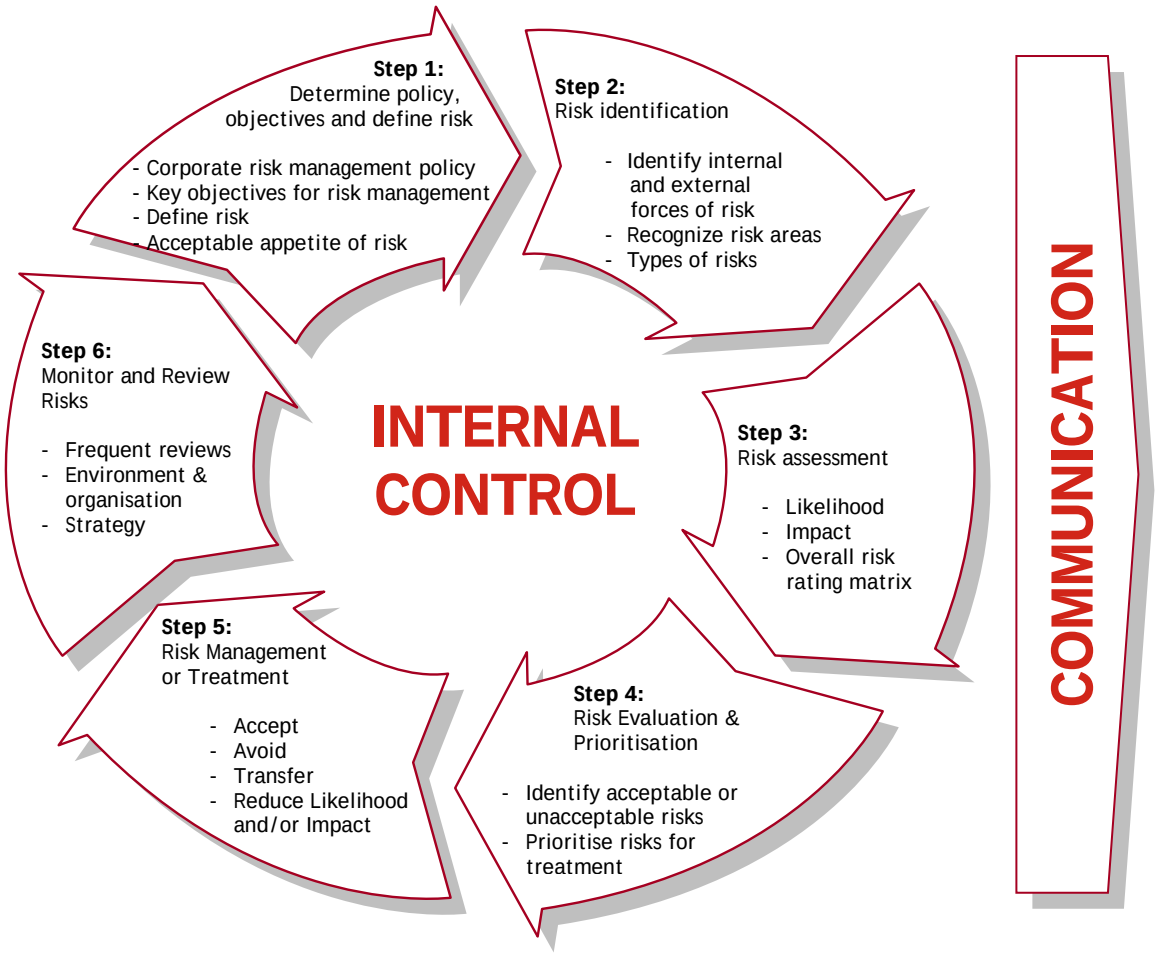
d. Applying the principles and processes of risk management at the conceptual stage of projects as well as throughout the project's lifetime.

e. Updating the risk registers within their area of responsibility for the onward consideration of the RMC.

# SECTION III: THE RISK MANAGEMENT PROCESS

Figure 1

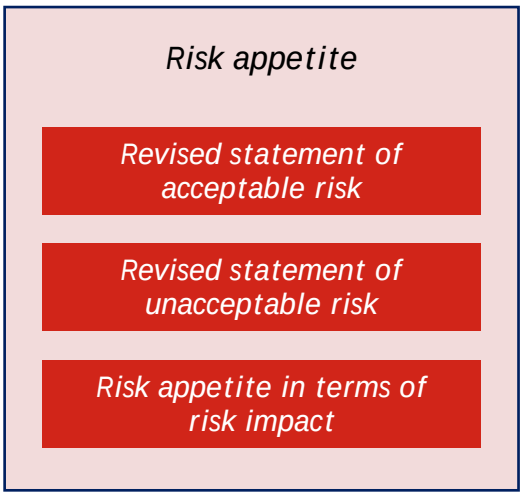
RISK MANAGEMENT FRAMEWORK DIAGRAM




A structured framework approach to risk management that incorporates all the necessary steps was developed. These steps are depicted in ***Figure 1*** above and described in the following pages.

## STEP 1: DETERMINE POLICY, OBJECTIVES AND DEFINE RISK

Risk analysis exercise is performed during the strategic planning process where strategic risks are identified based on past experience, industry trend and knowledge. The risks identified are considered for in the preparation of strategic plan analysis which in turn is used to guide the strategies to be adopted in order to achieve the business objectives and broad financial target of Prestariang Group.




| Input | Activity | Responsibility | Frequency | Output | Remarks |
|---|---|---|---|---|---|
| Past experience Industry trend and Knowledge | To identify key risk to be considered for SWOT analysis | Secretariat of respective Group Companies | Annually | Key risk for consideration in SWOT | Is to be conducted in conjunction with annual strategic planning exercise |

This step sets the tone for the RMC to ensure common understanding and objectives of the risk management process;

1. Vision, mission and objective.
2. Risk appetite.
3. Review and agreements of SWOT and STAPs as the focus and driver.

Prior to risk identification, the basis to which the risk management process will be applied is agreed upon, example: -

- Corporate and Division level – The business objectives
- Department and Operational levels – The core business processes
- Project level – The project goals, objectives and core activities

## STEP 2: RISK IDENTIFICATION

Risk identification is the process of determining and categorising the potential internal and external forces affecting the achievement of business objectives of Prestariang. It is a continuous process as risks and the environment are never constant but are subject to changes and uncertainties.

A variety of methods are available to assist in the identification process such as brainstorming sessions, control self-assessment questionnaires, interviews, etc.

Business model, outcomes of BOD/AC/RMC/Management meeting and workshop, strategic planning, Group Companies' risk flash report, risk register and internal audit review can be used as triggers to identify risks.

**Risk Identification Process**

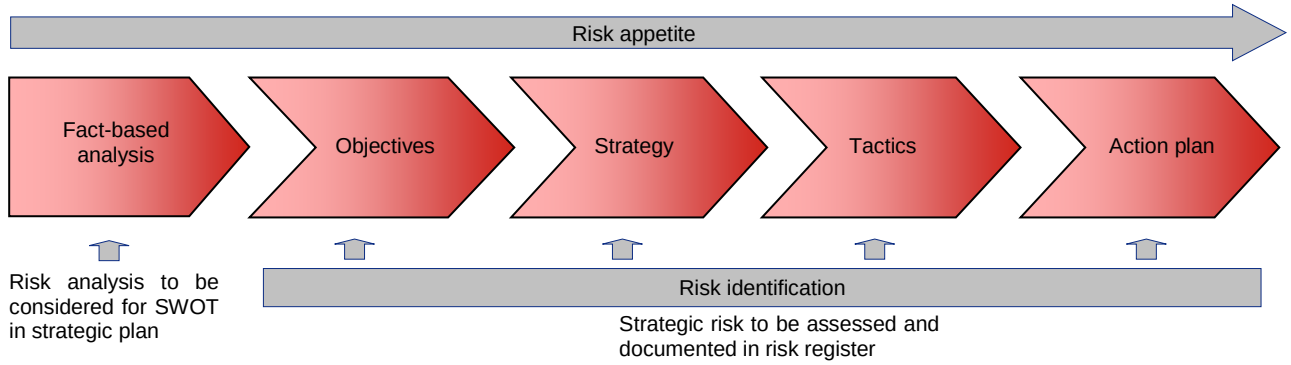
The process shall take into account the inter-relationships between the key processes, tasks and activities of Prestariang, the business culture and the relevant external forces.

Risk identification activities include, among others: -

- Analysis of the mission and objectives of Prestariang.
- Analysis of the strategies to achieve the objectives.
- Strengths, weaknesses, opportunities and threats ("SWOT") analysis.
- Analysis of financial statements.
- Analysis of a flowchart of the operations, which may alert unusual aspects of Prestariang's operations that give rise to special risks.
- Analysis of the organisation chart and reporting relationships.
- Analysis of existing corporate policies.

***Identifying Strategic Risk from STAPs***

The following diagram illustrates the process established to identify strategic risk affecting the Prestariang based on the selection of strategies, tactics and action plans ("STAPs"). Risk identified through this channel will be tracked and presented during the risk review meeting for a full risk assessment to be carried out. Subsequent to the risk assessment, risk action plan will be developed to mitigate the strategic risk that will prevent Prestariang Group from achieving its objectives.



**Risk Categories**

Within the Prestariang Risk Management Framework, risks are classified according to nine (9) main categories.

The following risk categories provide an indication of the internal and external forces of risk, risk areas and types of potential risks to be identified and managed, taking into account the inter-relationships between the key processes, tasks and activities of Prestariang, the business culture and the relevant external forces. This listing is not meant to be exhaustive and is primarily designed to facilitate the risk identification and assessment process.

| |
|---|
| **1 External**<br>External forces that could effect the achievement of the Company's business model. This includes climate change risks driven by changes in regulations, physical climate parameters and other climate-related developments. |
| **2 Perception**<br>How stakeholders' and public at large view the Company. |
| **3 Country**<br>Risks associated with doing business in other countries. |
| **4 Business & Strategic**<br>Risks affecting the industry and business model as a whole. |
| **5 Financial & Funding**<br>Company's ability to obtain, manage and finance its business operations. |
| **6 Customer & Product/Service**<br>Risks associated with customers and product/services. |
| **7 People**<br>Risks that are related to employees and employee issues. |
| **8 Internal Process Risks (including Information systems)**<br>The risks that operations are inefficient and ineffective. |
| **9 Technology**<br>Risk relating to technologies used in the company. |

## STEP 3: RISK ASSESSMENT

In risk assessment, each risk identified is assessed at two stages i.e. Gross and Net Risk.

- At Gross Risk level the identified risk is in its purest form without assigning any mitigating factors or controls. This is done so as not to prejudge the adequacy of current controls and to ensure objectivity.

- At Net Risk level the identified risk is re-rated taking into account the effectiveness of current mitigating factors and controls in place.

At both stages the identified risks are assessed in terms of their likelihood and impact.

### Risk Likelihood Assessment

Likelihood is the expected frequency of a risk occurring. To provide a more structured manner in assessing the likelihood of risk, it would be useful to assess how likely is it that the business will be exposed to a specific risk considering factors such as:

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

Best judgment should be made based on the table below and on the risk owner's management experience and intuition.

| | Likelihood description | |
|---|---|---|
| **Likelihood** | **Historical** | **Probability** |
| Certain | This risk is **expected** to occur in most circumstances. | More than 1 in 10 |
| Likely | This risk will **probably** occur in most circumstances. | 1 in 10-100 |
| Possible | This risk **might/should** occur at some time in the future. | 1 in 100-1,000 |
| Unlikely | This risk **could** occur at some time but doubtful. | 1 in 1,000 – 10,000 |
| Remote | This risk **may** occur but only in exceptional circumstances. | 1 in 10,000 – 100,000 |

**Risk Impact Assessment**

Impact (consequence) is the expected level of effect on the organisation of a risk occurring.

| | Impact description | | | |
|---|---|---|---|---|
| **Impact** | **Business Plans** | **Process & Systems** | **People** | **Reputation** |
| **Catastrophic** | Loss of ability to sustain ongoing operations. A situation that would cause a standalone business to cease operations. | Critical system failure, Bad policy advice or ongoing non-compliance. Business severely affected. | Death or multiple life threatening injuries. | Inquiry or adverse national media. |
| **Major** | Significant impact on the achievement of strategic objectives and targets relating to corporate plan. | Strategies not consistent with Government's agenda. Trends show service degraded. | Life threatening injury or multiple serious injuries causing hospitalisation. | Intense media scrutiny, e.g. front page headlines, TV, etc. |
| **Moderate** | Disruption of normal operations with a limited effect on the achievement of strategic objectives or targets relating to corporate plan. | One or more key accountability requirements not met. Inconvenient but not client welfare threatening. | Serious injury causing hospitalisation or multiple medical treatment cases. | Scrutiny required by external auditor or inquest. |
| **Minor** | No material impact on the achievement of business objectives or strategy. | Policy procedural rule occasionally not met or services do not fully meet needs. | Minor injury or First Aid treatment case. | Scrutiny required by internal audit to prevent escalation. |
| **Insignificant** | Negligible impact. | Minor errors in systems or processes requiring corrective action, or minor delay without impact on overall schedule. | Injuries or ailments not requiring medical treatment. | Internal review. |

**Risk Rating**

Based on the above assessment, risk rating is expressed in terms of combination of impact and likelihood. The combination is tabulated according to the following matrix for evaluation and prioritisation of risks.

| Likelihood | Insignificant | Minor | Moderate | Major | Catastrophic |
|---|---|---|---|---|---|
| Certain | M | S | S | H | H |
| Likely | M | M | S | S | H |
| Possible | L | M | M | S | H |
| Unlikely | L | M | M | S | S |
| Remote | L | L | M | M | S |

**Impact**

H = High S = Significant M = Medium L = Low

**Note :** *The integration of Risk Likelihood Assessment, Risk Impact Assessment and Risk Rating is summarised in Risk Assessment Matrix.*

**Types of Control**

| | |
|---|---|
| **Preventive** | These would include policies and procedures, organisation structure, budgets, delegated authorities, system access controls, segregation of duties, people development or training, security vetting for recruitment of sensitive positions, risk management framework, service standards or failure rates and service level agreements. |
| **Detective** | These are secondary checks and would include key risk indicators, reconciliations, signature verification process, validation checks, peer review, control self-assessment, management information systems, access security listing, and complaints. Various trigger points such as regulatory compliance ratios, also serve as detective controls. |
| **Corrective** | These would include business continuity plans, restructuring and re-engineering and operational damage control. |

**Determine Control Effectiveness**

Once the existing key controls have been identified, an assessment is made regarding the effectiveness of these controls to support Management of each risk. The following factors would assist the rating of the effectiveness of the key controls in managing the risk identified:

- Are roles, responsibilities and accountabilities defined and enforced?
- Is awareness communicated and followed?
- Are policies, procedures and guidelines defined and applied?
- Does existing controls and technology mitigate the key risk identified?
- Are existing auditing (internal and external audit) and other independent assurance functions adequate to detect internal control weakness or lapses?

Three control effectiveness assessments are used:

| | |
| --- | --- |
| **Satisfactory** | Controls are strong and operating properly providing a reasonable level of assurance that objectives are being achieved. |
| **Some weakness** | Some control weakness/inefficiencies have been identified. Although these are not considered to present a serious risk exposure, improvements are required to provide reasonable assurance that objectives will be achieved. |
| **Weak** | Controls do not meet an acceptable standard, as many weaknesses/inefficiencies exist. Controls do not provide reasonable assurance that objectives will be achieved. |

## Evaluating Risk In Terms of Inherent, Control or Project Risk

In evaluating the results from the analysis of risks, the risk could be segregated between inherent, control or project risk after which the nature of the risk are taken into account for selection of risk treatment strategy. The selection of risk treatment strategy is further explained in Step 5.

| | |
|---|---|
| **Inherent risk** | Risk that relate to the nature of the business and which are generally outside the control of Management |
| **Control risk** | Risk that a material error could occur and may not be prevented or detected on a timely basis by the system of internal control. Management can directly influence control risk |
| **Project risk** | Combination of inherent and control risk |

## Prioritise Risks for Treatment

In prioritising the results from the analysis of risk, risks should be ranked in terms of their significance to Prestariang after which the risks should be prioritised so that risk treatment strategy is focused on the areas of greater significance, within the risk appetite established. In this context, priority of treatment strategy is given to strategic risk identified during the annual strategic planning exercise.

| Risk Rating | Immediate action | Heightened action | On-going monitoring |
|---|---|---|---|
| High | | | |
| Significant | | | |
| Medium | | | |
| Low | | | |
| | Important and urgent status where treatment plan should commence immediately | Important and urgent status where treatment plan should commence within 3 months | Manage by routine procedures |

**Prioritisation**

Having identified and prioritised the risks, the next stage is to determine the treatment to the risks, as shown in the table below:

| | |
|---|---|
| **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.<br>*(It may not be possible to eliminate risk entirely and some net risk may still remain)* |
| **Accept** | Taking or increasing risk in order to pursue an opportunity and be prepared to manage its consequences/impacts.<br>*(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)* |
| **Transfer** | Sharing the risk with another party or parties e.g. through a contractual arrangement and risk financing. |

Risk treatment can create new risk or modify existing risks.

**Risk Treatment Plans – Documenting and Implementing Management Action Plans**

Based on the risk treatment strategy selected, specific risk treatment action plans are developed and prioritised based on risk assessment/ranking and prioritisation categories (e.g. immediate action, heightened action or on-going monitoring). The action plans developed should consider using the SMART[5] guidelines as appropriate.

The information provided in treatment plans should include:

- The reason for selection of treatment, including expected benefits to be gained;
- Those who are accountable for approving the plan and those responsible for implementing the plan;
- Proposed actions;
- Resource requirements including contingencies;
- Performance measures and constraints;
- Reporting and monitoring requirements; and
- Timing and schedule.

[5] Specific, Measurable, Achievable, Realistic and Time bound

## STEP 6: MONITORING AND REVIEW RISK

### Review

The RMC meets **quarterly** to review the changes to the overall risk profile that impacts the Prestariang Group. The result of this review should also form an integral part of the overall business planning process.

### Monitoring

On an ongoing basis the environment has to be scanned and consideration has to be given to any trends or factors relevant to the Prestariang. If there are any significant issues that impact the risk profile of the Prestariang or emerging risk being identified, immediate action should be taken to manage the risk by the risk owners.

## COMMUNICATION

The whole process of risk management must be communicated within the Prestariang Group.

Management who are responsible for strategic and operational decisions must be aware and apply the risk management process continuously.

Feedback to the RMC should be a continuous two-way communication in order for an effective and efficient risk management framework to prevail in the Prestariang Group.

Appropriate training in risk management should be given to enhance greater understanding and facilitate informed decision-making.

## INTERNAL CONTROL

Internal control is a process, enforced by the Board of Directors and the Management of Prestariang. It is designed to provide reasonable assurance regarding the achievement of Prestariang Group's objectives and to safeguard shareholders' investment and assets. Although it is impossible to provide complete assurance through any control system, the control systems must be designed and applied to manage the likelihood and impact of risk to acceptable levels.

Establishing an appropriate control environment is the responsibility of the Board and Management. The control environment is defined by the overall risk attitude, awareness and actions of Prestariang Directors and Management regarding the internal control system and its importance in the Prestariang Group.

**Internal Control System**

The internal control system[6] of Prestariang is made up of the following: -

- The risk assessment framework and activities.
- The control activities.
- The information and communication processes.
- The processes for monitoring the continuing adequacy and integrity of the internal control systems.

Additionally the internal control system should: -

- Be embedded in the Prestariang Group operations and form part of its culture.
- Be capable of responding quickly to evolving risks to the Prestariang Group's businesses arising from factors within the Prestariang Group and to changes in the business environment.
- Include procedures for reporting immediately to appropriate levels of management any significant control failures or weaknesses within the Prestariang Group that are identified together with details of corrective action being undertaken.

**Link between Risk and Internal Control**

In determining the policies with regard to sound internal controls, the following factors should be considered: -

- The adequacy of the whole risk management framework.
- The nature and extent of risks facing the Prestariang Group.
- The risk appetite/tolerance, which is regarded as acceptable for the Prestariang Group to bear.
- The likelihood of the risks concerned materialising.
- The ability to reduce the incidence of risks that do materialise and their impact on the Prestariang Group.
- The costs of operating particular controls relative to the benefit thereby obtained in managing the related risks.

[6] Based on the Committee of Sponsoring Organisations of the Treadway Commission (COSO) "Internal Control - Integrated Framework model"

**Periodic Review of the Adequacy and Effectiveness of the Internal Control System**

In reviewing the adequacy and effectiveness of the internal control system the following shall be taken into consideration: -

- Ensuring an appropriate organisational structure for planning, executing, controlling and monitoring business operations with appropriate authorisation limits.
- Reviewing the consolidated risk register of the Prestariang Group and receiving regular reports on any significant problems that have occurred during the year and changes to the risks over the period under review.
- Reviewing external and internal audit work plans and their results.
- Reviewing periodically the long-term financial objectives and business strategies of the Prestariang Group.
- Reviewing variance reports from major operating subsidiaries and associates against business objectives.
- Effectively applying policies, processes and activities relating to internal control and risk management through control self-assessments and internal audit reviews.

**Control Risk Self Assessment**

Control risk self assessment is defined as 'a methodology used to review key business objectives, risks involved in achieving the objectives and internal controls designed to manage those risks[7]'.

It is envisaged that with the growing experience and knowledge of an effective risk management process, management (particularly department heads) and other risk owners will be able to identify and assess risks at their functional level. This will lead to risks being naturally identified, anticipated and treated at the beginning of any project or undertaking and used as a tool in assessing their viability.

[7] "A Perspective on Control self-Assessment" by the Institute of Internal Auditors

# ANNEXURE

ANNEXURE 1

## RISK ASSESSMENT MATRIX

| | | IMPACT | | | | |
|---|---|---|---|---|---|---|
| | **Reputation** | Internal review. | Scrutiny required by internal audit to prevent escalation. | Scrutiny required by external auditor or inquest. | Intense media scrutiny, e.g. front page headlines, TV, etc. | Inquiry or adverse national media. |
| | **People** | Injuries or ailments not requiring medical treatment. | Minor injury or First Aid treatment case. | Serious injury causing hospitalisation or multiple medical treatment cases. | Life threatening injury or multiple serious injuries causing hospitalisation. | Death or multiple life threatening injuries. |
| | **Process & Systems** | Minor errors in systems or processes requiring corrective action, or minor delay without impact on overall schedule. | Policy procedural rule occasionally not met or services do not fully meet needs. | One or more key accountability requirements not met. Inconvenient but not client welfare threatening. | Strategies not consistent with Government's agenda. Trends show service degraded. | Critical system failure, Bad policy advice or ongoing non-compliance. Business severely affected. |
| | **Business Plan** | Negligible impact. | No material impact on the achievement of business objectives or strategy. | Disruption of normal operations with a limited effect on the achievement of strategic objectives or targets relating to corporate plan. | Significant impact on the achievement of strategic objectives and targets relating to corporate plan. | Loss of ability to sustain ongoing operations. A situation that would cause a standalone business to cease operations. |
| | | **Insignificant** | **Minor** | **Moderate** | **Major** | **Catastrophic** |
| **LIKELIHOOD** | **Certain** (>1 in 10 — Is expected to occur in most circumstances) | **Medium** | **Significant** | **Significant** | **High** | **High** |
| | **Likely** (1 in 10 - 100 — Will probably occur) | **Medium** | **Medium** | **Significant** | **Significant** | **High** |
| | **Possible** (1 in 100 - 1,000 — Might/should occur at some time in the future) | **Low** | **Medium** | **Medium** | **Significant** | **High** |
| | **Unlikely** (1 in 1,000 - 10,000 — Could occur at some time but doubtful) | **Low** | **Medium** | **Medium** | **Significant** | **Significant** |
| | **Remote** (1 in 10,000 - 100,000 — May occur but only in exceptional circumstances) | **Low** | **Low** | **Medium** | **Medium** | **Significant** |