Risk Management Policy & Procedure Document

Contents

Appendices

Appendix A: Guidance on risk treatment options

Appendix B: Risk categories

Appendix C: Risk parameters

Appendix D: Template for risk workshop preparation

Appendix E: Risk register

Abbreviations

AC	-	Audit Committee
Sunway or the Company	-	Sunway Berhad
Board Committee	-	Sunway's Board of Directors Committee
BOD	-	Sunway's Board of Directors
BSC	-	Balanced Scorecard
CEO	-	Chief Executive Officer
CRO	-	Chief Risk Officer
ERM	-	Enterprise risk management
RMC	-	Risk Management Committee
HOD	-	Heads of Division/ Department
MD	-	Managing Director
PLC	-	Public Listed Company
RC	-	Risk Coordinator
RMP&P/ document	-	Risk Management Policy and Procedures document
SIC	-	Statement on Internal Control
the Group	-	Sunway and its subsidiaries and significant associates

Key Terms

Establishing a common language for risk is important in promoting the practice of a consistent and effective risk management across the diverse activities of Sunway Group. The terms used in this manual are listed below, together with practical descriptions of their meaning.

ERM framework
A structured and disciplined approach aligning strategy, processes, people, technology and knowledge with the purpose of evaluating and managing the risks an organisation faces as it seeks to create value – in essence every employee is part of the Group risk management framework.

Gross risk
The level of impact and likelihood of a risk before consideration of the control or risk mitigation is applied.

Key risks
Those risks that have been assessed as being most critical to impact the achievement of Group's business objectives.

Likelihood of occurrence
Probability that a particular risk will occur. Probabilities range from rare to almost certain and are evaluated against a defined time period.

Management
Consists of management personnel in Sunway, subsidiaries and associates.

Objectives
Description in measurable terms of what must be accomplished in order to reach the Group's goals.

Net (residual) risk
The remaining level of risk after risk treatment or controls have been applied.

Risk
Risk is the effect of uncertainty on the objectives.

NOTE 1 An effect is a deviation from the expected — positive and/or negative.
NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).
NOTE 3 Risk is often characterized by reference to potential **events** and **consequences**, or a combination of these.
NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated **likelihood** of occurrence.
NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.
(Source: ISO 31000: 2009 – Risk Management Principles and Guidelines)

Key Terms (cont'd)

Risk impact/ consequences
An evaluation of the significance of a particular risk to the organisation. Magnitude of impact is determined with respect to the organisation's appetite and capacity for risk, and organisational objectives.

Risk appetite
Risk appetite is defined as the level of risk Sunway is prepared to accept to achieve its objectives measured in terms of variability of return (i.e. risk) in order to achieve a desired level of result (i.e. return) as set out in the risk parameters.

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

Risk management policy
Document outlining the vision, objectives, principles and guidelines for risk and assurance in the Group.

Risk management representative
Individual(s) within the Group consisting the Risk Coordinator and Risk Assistant who are responsible for coordinating risk management activities within their operating divisions, subsidiaries and associates.

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

Risk parameter
Used to estimate the consequences of a risk should it occur and will be based on Sunway' "risk appetite".

Stakeholder
Any individual or group, internal or external, with an interest in the Group, including:

- Shareholders
- Customers
- Bankers
- Directors
- Business/ Joint Venture partners
- Suppliers
- Employees
- Government agencies/ regulators
- Community

Policy statement

Sunway is committed to integrating risk management practices into all business processes and operations to drive consistent, effective and accountable action, and management practices.

Sunway recognises that risk is dynamic and is inherent in all external and internal operating environments and is committed to managing risks effectively. Just as risk is inherent in our operations, risk management is also inherent in all decision making and management processes.

Effective risk management provides the mean for achieving competitive advantage and is pivotal to safeguarding assets, enabling the on-going growth and success of our business. To meet this commitment, risk management is to be every employee's business. All employees are responsible and accountable for managing risk within their area of responsibility.

It is important that Sunway have a robust Risk Management Framework in which critical risks are proactively identified, communicated and managed across the organisation. Sunway's fundamental, underlying risk management principles are consistent with the ISO 31000 Risk Standards; and COSO framework for Enterprise Risk Management. Management is committed to the 'best practice' risk management practices across the business, in Malaysia and international scenes.

Risk management is a priority and will be implemented through consultation with the Board, President, Directors, Executives and all employees.

Risk Management Committee
Date: _____

1. Introduction

This risk management policy and procedure document ("document") is designed to:

- establish the context for an embedded Enterprise Risk Management ("ERM") framework within Sunway Berhad ("Sunway" or "the Company"), its subsidiaries and significant associates ("Sunway Group" or "the Group");
- formalise the ERM functions across Sunway Group;
- sensitise staff more strongly to risk identification, measurement, control, ongoing monitoring, responsibilities and accountabilities;
- coordinate and standardise the understanding and application of ERM within Sunway Group; and
- ensure compliance by Sunway's Board with its organisational obligations and duties of care in accordance with the Malaysian Code on Corporate Governance ("MCCG") and the Listing Requirements ("LR") of Bursa Malaysia Securities Berhad.

This document is a **corporate policy** applicable to Sunway Group. It defines the standard conditions and minimum requirements for ERM by the Company, all its subsidiaries and significant associates.

1.1 Objective

The objectives of the Group's risk management policy and procedure document are to:

- outline the Group's risk context which comprises group's philosophies, strategies and policies, and operating system so as to better manage the business risks faced by the Group;
- provide guiding ERM principles to Heads of Division to govern the action of their operating personnel pertaining to risks; and
- provide assurance to the Board that a sound risk management and internal control system is in place and in accordance with the regulatory bodies' requirements.

This document shall be reviewed periodically to ensure that it is always consistent with the business and market environment that Sunway Group is faced with.

To realise the Group's ERM objectives, we will:

- ensure that an appropriate ERM framework is in place and that it is aligned to Sunway's business strategy;
- support the framework and strategy with an appropriate organisational structure and ensure that associated responsibilities are clearly defined and communicated at all levels;
- ensure the risk management process is applied systematically across the Group to identify, assess, treat and manage risks that threaten resources or the achievement of objectives;
- ensure that risk information is communicated through a clear and robust reporting structure; and

- integrate ongoing ERM activities within the business of the Group.

1.2 Benefits

The benefits to be derived from an effective ERM framework include the following:

- a platform to enable Sunway Group to anticipate and respond to risks effectively;
- encourages comprehensive and reliable sources of information on status of risks and controls;
- minimisation of the likelihood of unexpected damage to the Group's financial performance, reputation and stakeholder confidence;
- the opportunity to align corporate strategy with risk strategy;
- a tool which allows management of risks affecting both tangible and non tangible assets;
- an opportunity to eliminate cost through more targeted and effective controls that are aligned to key objectives and risks;
- provides the basis for more effective strategic planning;
- contributes to improved organisational efficiency and effectiveness;
- enables optimum use of resources;
- provides Management with a concise summary of the major risks affecting the Group and a mechanism to ensure that appropriate resources are directed towards areas of high risk; and
- provides a framework for ensuring that unavoidable risks are adequately managed.

1.3 Restriction

This RMP&P is not for general circulation nor is it to be reproduced, either in part or in full, or used for any other purpose without Management's prior written consent. The Management does not assume any responsibility or liability arising from any losses however occasioned by any other party because of circulation, publication, reproduction or use of this document.

1.4 Definition of risk

Risk may be viewed as "the effect of uncertainty on the objectives", thus, includes threat of certain events, action or loss of opportunity that, if it occurs or crystallises, will adversely affect any or a combination of the following:

- value to Sunway's shareholders and other stakeholders;
- ability to achieve objectives;
- ability to implement business strategies;

- manner in which operations are conducted; and
- Sunway's reputation.

As may be appreciated from the concept and due to the diversity of business objectives, strategies and operations, a multitude of risks would be faced by an entity. These may be categorised in general into strategic risks, operational risks and project risks, which are dealt with in Section 1.9. Because the future as such is uncertain, any business activity is associated with risks and rewards, and it's very objectives are to identify and reap rewards and opportunities, as well as to manage and control the resulting risks.

1.5 Definition of Enterprise Risk Management

ERM is a structured and disciplined approach aligning strategy, processes, people, technology, and knowledge with the purpose of evaluating and managing the risks the Group faces as it creates value.

"Enterprise-wide" means the removal of traditional functional, divisional, departmental, or cultural barriers. A truly holistic, integrated, future-focused, and process-oriented approach helps the Group manage all key business risks and opportunities with the intent of maximising shareholder value for the Group as a whole.

ERM shall be a core management competency that incorporates a well-structured systematic process to identify business risks and lessen their impact on the Group.

This involves the following core elements:

- the identification of each business risk;
- the measurement of the identified business risk;
- the control or the way the risk is managed in line with the needs of the Sunway Group's policies and strategies; and
- constant monitoring and communicating of risks associated with any activity, function or process in a way that will enable the Sunway Group to minimise losses and maximise opportunities.

The risk management framework, as shown in Diagram A below, provides a holistic view of how risks and strategies are linked to a performance management system such as Balanced Scorecard ("BSC") in order to achieve the Group's business objectives. It also assists in identifying changes and efforts required to embed an effective risk management process. Further information on the integration of ERM is explained in Section 7 of this document.

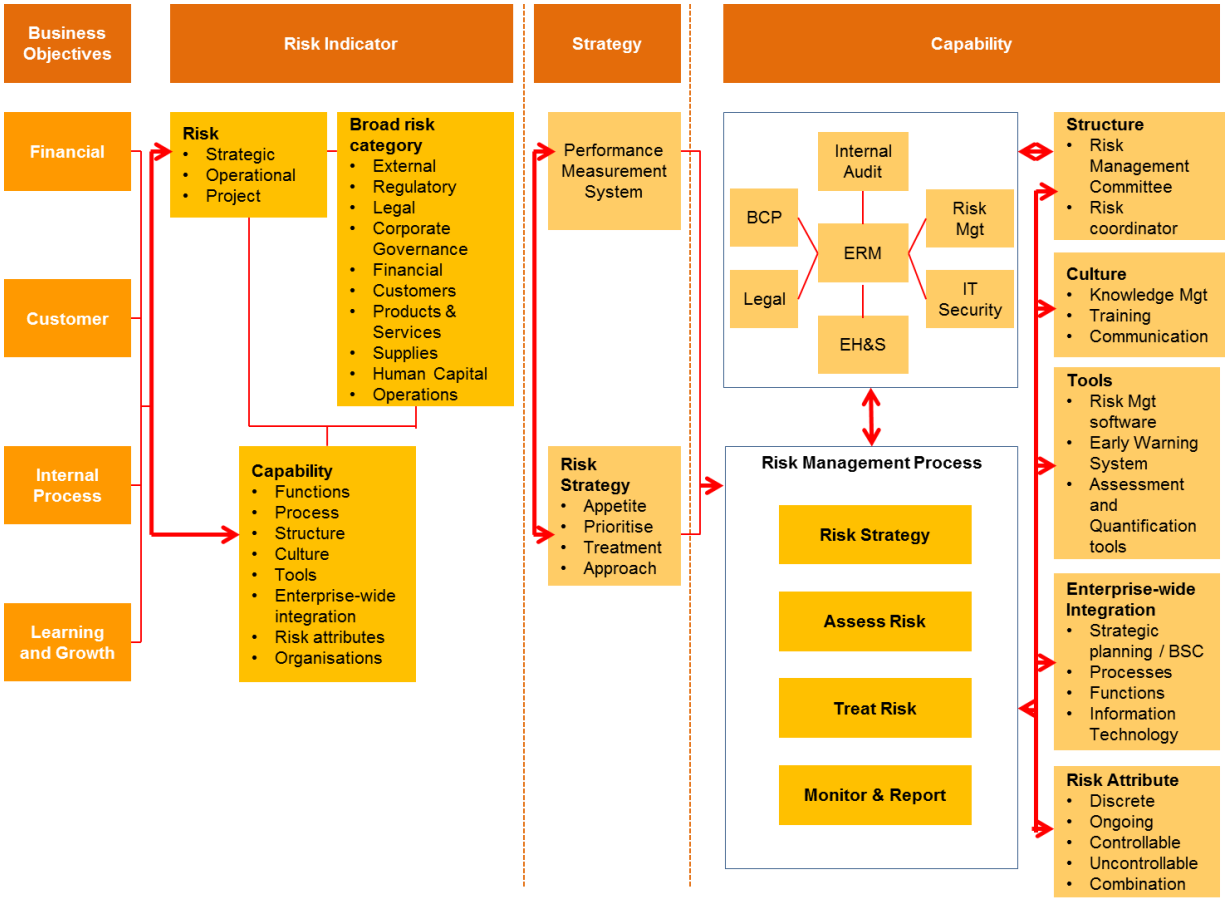


Diagram A: An integrated ERM framework with BSC.

The risk management framework provides the basis for challenging the maturity of risk management in organisations and assists with identifying practical and relevant steps to move along the maturity continuum depending upon the desire to change within the organisation.

In this context, the ERM framework that Sunway could adopt would consist of five elements, which is in line with globally accepted risk standards such as the ISO 31000 Risk Management Principles, as depicted in Diagram B below:

Framework Element	Description
Risk Governance	Establish an approach to developing, supporting and embedding the risk strategy and accountabilities
Risk Assessment	Identify, assess, and categorise risks across the enterprise
Risk Quantification and Aggregation	Measure, analyse and consolidate risks
Risk Monitoring and Reporting	Report, monitor and conduct activities to provide insight risk management strengths and weakness
Risk and Control Optimisation	Use risk and control information to improve performance

Diagram B: Five key elements of ERM Framework

1.6 Factors demanding the management of risk

The global pace of change, resource constraint, demands from stakeholders for growing openness, transparency and accountability and continued pressures for organisational change, all has an impact on the Sunway Group. These factors demand Sunway Group to have a more systematic risk management structure.

Broadly, the benefits of managing risk include the following:

- early exploitation of business opportunities;
- increased likelihood of achieving business objectives;
- recognised the upside of the risk;
- increased market capitalisation;
- more effective use of management time; also avoid “fire-fighting”;
- lower cost of capital;
- fewer unexpected threats to the business;
- more effective management of change; and
- clearer strategy setting.

By consciously and regularly looking for “what else might happen” scenarios, and by discovering possible unintended consequences in advance of choosing a particular course of action, our decision-making will obviously be based upon more relevant and complete information, and we will significantly decrease the chances of being “blindsided” by some unforeseen scenarios or potential crises. We will also have better contingency plans prepared should one of the risk scenarios materialise.

1.7 Listing requirements for risk management

The Listing Requirements of Bursa Malaysia, Chapter 15 of the LR sets out the key corporate governance requirements for PLCs.

In effect, the Malaysian Code on Corporate Governance (“MCCG”) was given its practical efficacy through the key provisions in the LR on corporate governance disclosure requirements in the annual reports of PLCs:

The main requirement is for the BOD to maintain a sound system of internal control within the PLC group through a system of internal control where the monitoring of risks and controls is embedded into the fabric of the Group through the implementation of an ERM system which balances risks and controls.
This ERM system is supplemented by an objective assurance on the adequacy and integrity of the internal control system provided by an independent internal audit function.

1.8 Critical success factors for risk management

The successful management of risk within the Group will depend upon:

- risk management being an integral part of strategic, project and operational planning and activities throughout all levels of the Group;
- risk management being openly accepted and supported by the Group's leadership as providing good business value, with this acceptance reinforced through avenues such as managers and staff performance requirements and part of their performance assessment criteria; and
- risk management being easy to incorporate into our daily activity and being seen as helpful to us in achieving our vision and strategic goals.

1.9 Risk management context and accountabilities

The context within which we manage our risks and the key focus of accountability for this is as follows:

1.9.1 Strategic risk

Strategic risks are primarily risks caused by events that are external to the Group, but have a significant impact on its strategic decisions or activities.

The causes of these risks include such areas as national and global economies, government policies and regulations, inflation, geopolitical changes, interest rates, and climatic change. Often, they cannot be predicted or monitored through a systematic operational procedure. The lack of advance warning and frequent immediate response required to manage strategic risks means they are often best identified and monitored by senior management as part of their strategic planning and review mechanisms.

Accountability for managing strategic risks therefore rests with the Board and the President. The benefit of effectively managing strategic risks is that we can better forecast and quickly adapt to the changing demands that are placed upon the Group. It also means that we are less likely to be surprised by some external event that calls for significant change.

1.9.2 Operational risk

Operational risks are inherent in the ongoing activities within the different business units or subsidiaries of the Group. These are the risks associated with such areas related to the day-to-day operational performance of staff, the risks caused by the company structure and the manner in which the subsidiaries report to corporate headquarters. Senior management needs ongoing assurance that operational risks are identified and managed.

Accountability for managing operational risks rests particularly with the Heads of Divisions, Departments and Business Units. The benefits of efficiently managing operational risks include maintaining superior quality standards, eliminating undesirable surprises, the early identification of problematic issues, being prepared for emergencies if they happen and being held in high regard by shareholders for the efficient and effective management of risk.

1.9.3 Project risk (including acquisitions and investments)

These are risks associated with projects that are of a specific, normally short term nature and are frequently associated with acquisitions, change management and integration projects. An effective strategy for managing project risks is to develop a set of key criteria to manage the significant risks that are common within most projects. This approach assists Project Managers with the identification of the risks inherent in individual projects.

Project Sponsors are accountable for the achievement of project deliverables and outcomes. However, specific risks associated with project management are normally

delegated to project managers for attention and action. Included among the benefits of efficiently managing project risks are the avoidance of unexpected time and cost overruns. Additionally, when project risks are well managed there are fewer integration problems with assimilating required changes back into general management functions.

2. Risk management strategy and policy of Sunway Group

2.1 Risk strategy

Risk management strategy is an integral component of overall Group strategy, which determines core capabilities, divisions, competitive advantages, the formation of the value-added chain, and thus the Group's value drivers. The risk management strategy will align ERM resources and actions with business strategy necessary to maximise organisational effectiveness. Linking the business strategies to ERM can also provide a context for setting risk appetite and risk measures so that they are linked to the strategic plan of the Group.

As an essential facet of the risk management system, the following risk strategy forms the strategic thrust of the ERM framework and sets the risk management tone that guides all employees of the Group in dealing with risks in a rational, target-oriented manner:

- Sunway's risk management policy statement shall be adopted by all business units and divisions and the risk management decisions shall be made at the operating level where knowledge and expertise reside. Responsibility for risk management will be undertaken by business units/divisions with appropriate advisory guidelines from the Risk Management Committee;
- the Board strongly supports risk management with formal reporting. Risk management is periodically on the Board's agenda, and the Board and senior management are aware/ trained on risk;
- this document shall define and document the Sunway Group's risk management policy, procedures and objectives, which are part of a wider ERM framework, and communicated across the Group;
- risk management is linked to business and operational planning, and is generally incorporated into new projects; and
- the risk management process is meant to promote a proactive risk management approach and create the necessary risk awareness and cultivate an intra-group risk and control culture.

Just as a business strategy indicates the direction of the business, a risk strategy provides guidance for the risk activities within a company. It can set the tone for aggressive or conservative risk management activities, dictate how measuring and monitoring activities can be carried out and provide the "bird's-eye" view needed by management and the board. Indeed, it is the risk strategy that provides the backbone for embedding risk management within the culture of the business.

2.2 Risk management policy

The following outlines the Sunway Group's risk management policies:

- to weigh business decisions against the philosophy that business risks would be deliberately incurred if the associated rewards are expected to enhance the Group's shareholder value;
- to ensure risks which may have a significant impact upon the Group are identified in a manner which would result in their expeditious treatment;
- to provide reasonable assurance to the Group's stakeholders that the probability of attaining its objectives would be enhanced by the establishment of an ERM framework;
- to establish an environment or platform whereby risk management activities may be effectively undertaken;

- to manage risks by adopting best practice methodologies for the identification, analysis, evaluation, reporting, treatment and monitoring of risks; and
- to provide an assurance regarding the extent of its compliance with regulatory requirements and the policies and procedures contained within this document.

The Group will communicate and provide the necessary resources, structures, system and training to ensure this policy is understood, implemented and maintained at all levels. All employees are responsible for managing risks.

2.3 Applicability

This policy, including the attached procedures, applies to the Group, management and staff, with immediate effect.

3. Risk structure

3.1 General concepts

Risk management cannot function effectively in isolated silos. An appropriate framework has to be established within the Group to provide the control environment for risk management activities. This framework or structure should be embedded within the fabric of the Group.

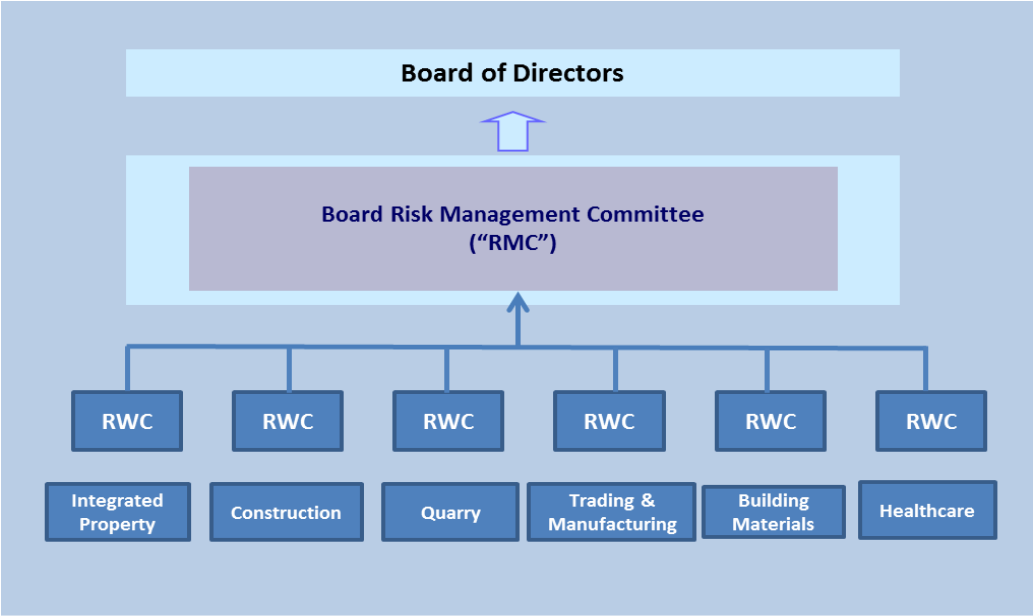
Key elements in the risk management structure include the following:-

- risk management organisational structure – the establishment of management committees and forums (refer to Section 3.2);
- roles, responsibilities and accountabilities ("RRA") of individuals and teams – the RRA should be clearly defined and communicated at the Group level. Individual RRA should be included within the job description and used as a performance indicator;
- risk function – a centralized risk function should be independent from day-to-day operations and management. A Chief Risk Officer may be appointed to head the centrailsed risk function and act as the risk coordinator to oversee the risk management process. He/ She may also be involved in other corporate initiatives, eg. Human Resource, Legal, IT, etc.
- use of common risk terminology – involves the establishment of common Group wide risk terminology which are clearly defined and communicated to all employees. Key features relating to terminology are covered under Chapter 4 (Risk assessment process);
- reporting structures – this is a crucial element. Risk reporting should be continuous and embedded into existing management reporting processes and structures. The frequency, format and level of reporting should be formalised, with a system to allow red flags or high risk areas to be immediately channeled to the appropriate level for action. Chapter 5 focuses on risk reporting;
- technology (integration) – technological products should be used to capture salient risk information for the purposes of consolidation, reporting and monitoring;
- awareness culture and appropriate skill sets – risk should be part and parcel of the working culture. It should be understood within all aspects of everyday business management. The desired culture should be demonstrated by the Board and senior management and applied consistently;
- performance incentive systems – risk management should be seen as a core competency for all employees and incorporated into performance appraisals; and
- training and education programmes on risk management – this should be a mandatory requirement for all employees, with varying degrees of emphasis depending on seniority. The training program should be woven into standard management training.

This document shall focus on the organisational and reporting elements of the risk structure. The human resource and technological aspects would be outside the scope of the document. It should be emphasised however that the document may form a principal ingredient in risk training and awareness sessions.

3.2 Risk organisation structure

A risk organisational structure as illustrated below is established for effective risk management:



3.2.1 Board of Directors

Sunway's Board of Directors retains the overall risk management responsibility in accordance with Best Practices Provision AAI in Part 2 of the MCCG, which requires the Board to identify principal risks and ensure the implementation of appropriate systems to manage these risks.

The principal roles and responsibilities of the Board in risk management are as follows:

- determine risk management policy;
- approve risk management philosophy;
- overall risk management oversight;
- communication with external shareholders and other stakeholders; and review the risk profile of the Group.

The Board shall approve the risk management strategies but will delegate authority for day-to-day decisions to the Risk Management Committee.

3.2.2 Risk Management Committee ("RMC")

A RMC should be established at the Group level which shall meet at least 4 times a year. Meetings can be conducted at more frequent intervals should conditions require.

Its principal roles include the following:

- reviewing and recommending risk management strategies, policies and risk appetite/ tolerance for board's approval;
- reviewing and assessing adequacy of risk management policies and framework in identifying, measuring, monitoring and controlling risk and the extent to which these are operating effectively;

- ensuring infrastructure, resources and systems are in place for risk management; ensuring that the staff responsible for implementing risk management systems perform those duties independently of the business units' risk taking activities;
- reviewing management's periodic reports on risk exposure, risk portfolio composition and risk management activities;
- reviewing the enterprise risk rating and determine the critical risks to be escalated to the Board on a quarterly basis; and
- working with Group Chief Financial Officer and Group Internal Audit, contribute to the preparation of the Statement on Internal Control for inclusion in the Company's Annual Report, and to recommend the same for the approvals of the Audit Committee and Board.

Significant risk issues evaluated by the RMC and/or major changes proposed by this committee will be discussed at Sunway's Board meeting. The RMC in turn is assisted by the Chief Risk Officer who acts as the coordinator.

In the scope of the risk management policies set out in this document, the RMC of Sunway is primarily responsible for review of the risk management process. The same principle applies analogously to the Risk Working Committee, where risk rests with the Risk Working Committee of the respective business units.

3.2.3 Risk Working Committee ("RWC")

The RWC is established at the business unit level and shall meet at least four times a year. Meetings can be conducted at more frequent intervals should conditions require.
RWC is led by the PCMs and members may be nominated employees from Finance, Business Development, Human Resources, Project Management, a designated Risk Coordinator and others as deemed appropriate.

The RWC's principal roles and responsibilities are as follows:

- identify and communicate to the Board of the subsidiary (if applicable) and the RMC the critical risks (present or potential) the subsidiary's business unit faces, their changes, and the management action plans to manage the risks;
- communicate risk management requirements in the subsidiaries and business units;
- review risk profiles and performance for the business units; and
- review and update the business unit's risk management methodologies applied, specifically those related to risk identification, measuring, controlling, monitoring and reporting.

Significant risk issues evaluated by the RWC and/ or major changes proposed by this committee will be discussed at management meeting and also the meetings convened by the RMC.

In essence, risks are dealt and contained at the respective business unit level, and are communicated upwards to Sunway's RMC through each subsidiary's board, or RWC, as the case may be. The subsidiary's board may delegate the reporting function to the RWC of their business unit, but they shall retain the overall risk responsibility.

3.2.4 Chief Risk Officer (CRO)

A CRO (who is primarily accountable for the effectiveness of the risk management system) should be distinguished from a risk owner, the latter being such person within the Group who is able to actively influence the identified risk through decisions and actions. A

CRO leads the Group Risk Management Department and should be supported by a risk management team.

The following functions and duties are incumbent on a CRO:

- acting as central contact and guide for ERM issues within the Group;
- coordinating the issuance of group-wide uniform ERM standards, combined with the authority to set guidelines with the approval of Sunway's RMC;
- coordinating ERM routinely within the Group;
- supervising ERM policy implementation at the Group level;
- developing and updating the ERM system at the Group level after consulting with Sunway's RMC;
- documenting the ERM system at the Group level;
- aggregating the Group's risk position and yearly reporting to the Board on the risk situation/status;
- training and communicating ERM details within the Group;
- participating in business planning activity to allow for consideration of risks in business plans and budgets;
- monitoring progress of action plans to address key risks identified. Risk action plan on key risks should be linked to performance management system such as the BSC initiatives; and
- liaising with risk owners on risk action plan.

3.2.5 Day to day risk management

The day-to-day risk management resides with the respective business units. These business units are either:

- the individual corporate departments for centralised functions/ processes (finance, legal and secretarial, human resources, etc) of the Group, under the responsibility of the Board; or
- the individual business units or operation, under the responsibilities of the Heads of the Business Units; or
- the subsidiaries and significant associates of Sunway, under the responsibilities of each subsidiaries' board or equivalent.

The business unit's management is accountable for the comprehensiveness of the risks identified, their assessment, as well as their bottom-up reporting. Actively managing risks is the key duty of any manager. Managers shall assist risk owners in identifying, measuring, controlling, monitoring and reporting risks and have both the right and obligation to contribute to risk management.

The principal roles and responsibilities of the business unit's management are as follows:

- manage business unit's risk profile;
- report risk exposures to the respective RWCs;
- develop and implement action plans to manage risks;
- report status of action plans to the CRO; and
- ensure critical risks are considered in the management plan.

3.2.6 Internal audit function

Internal auditing is an independent, unbiased function, which contributes by means of auditing and consultancy to the proper assessment of the risk situation, vulnerability, value enhancement and business process improvement.

As such, the internal audit function is involved in validating the results of the ERM processes. The group internal audit function would examine the risk management systems for the completeness, comprehensiveness, and reliability, besides verifying the ERM system for adequacy and effectiveness.

The principal roles and responsibilities of the internal audit function are as follows:

- provides assurance to the Sunway Audit Committee on the adequacy and integrity of the internal control systems in place to manage risks across the Group and provides an independent challenge to the Sunway Group and its operating divisions, to ensure the principles and requirements of managing risk are consistently adopted throughout the Group;
- provides the Group with a third line of defence on risk management. In conjunction with the Audit Committee, it provides an independent assurance to the BOD on the ERM system and validation of internal control procedures;
- the principal reporting responsibility of the Group Internal Audit department is the periodic internal audit activity report and follow-up reviews of the Group's system of internal control to the Audit Committee;
- ensures the quality of internal audit work and that audit reports address key risks, and the proposed improvement recommendations that are pragmatic and effectively communicated to the right level of personnel; and
- provides the Audit Committee an annual risk-based internal audit strategy (if applicable).

3.3 Responsibility for risk management

While managers are accountable for risk management at their particular level, responsibility for good risk management rests with every staff member. This includes going about jobs in a careful and conscientious manner that contributes to the high ethics and culture within the Group.

The individual accountability for risk management responsibilities has been addressed by the applicable laws and regulations that bind management and staff, as well as by each Company's memorandum and articles of association, internal policies and procedures, limits of authority, individual employment contracts, the general corporate policies and the guidelines for specific operations, divisions or business units.

3.3.1 The role of risk owners

Risk owners are the PCMs/UPCMs/HODs/ process owners who are directly responsible for the day-to-day operations of their respective units. The concept of risk owners is also extended to project leaders of routine or ad hoc projects. The roles and responsibilities of these identified risk owners are:

- identification, assessment and implementation of action plans to address risks arising from operations;
- assigning ERM responsibilities and accountabilities within their respective departments or teams;
- reporting to the RMC of all risks with significant impact and progress of action plans taken to manage the risks;
- taking immediate actions on all unacceptable risks;
- reviewing the effectiveness of existing controls and risk mitigating strategies; and
- submitting periodic reports and risks faced by the respective departments/ projects to RWC and RMC.

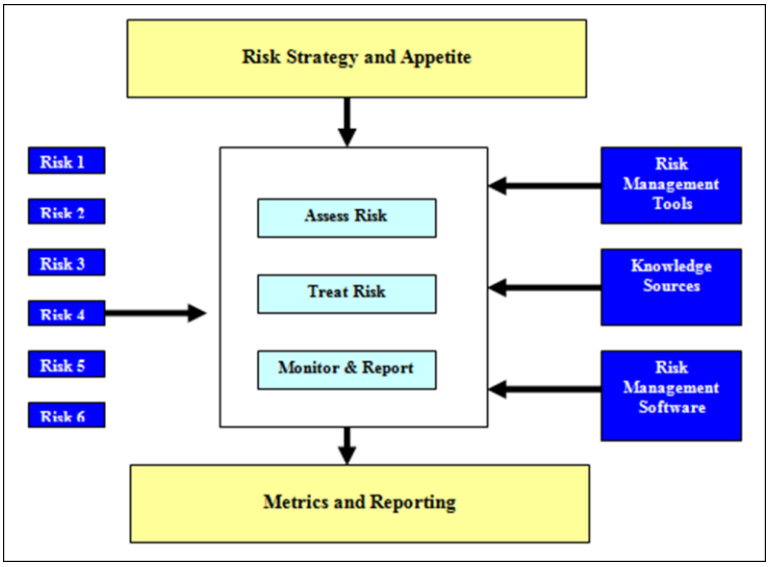
3.3.2 The role of all Sunway employees

- have a general duty of care and are responsible for complying with requests from Management in connection with the application of this Policy;
- conscious of the risks related to their actions and decisions; and
- through appropriate preventive actions, all reasonable care should be taken to prevent loss, to maximise opportunity and to ensure that Sunway's operations, reputation and assets are not jeopardised.

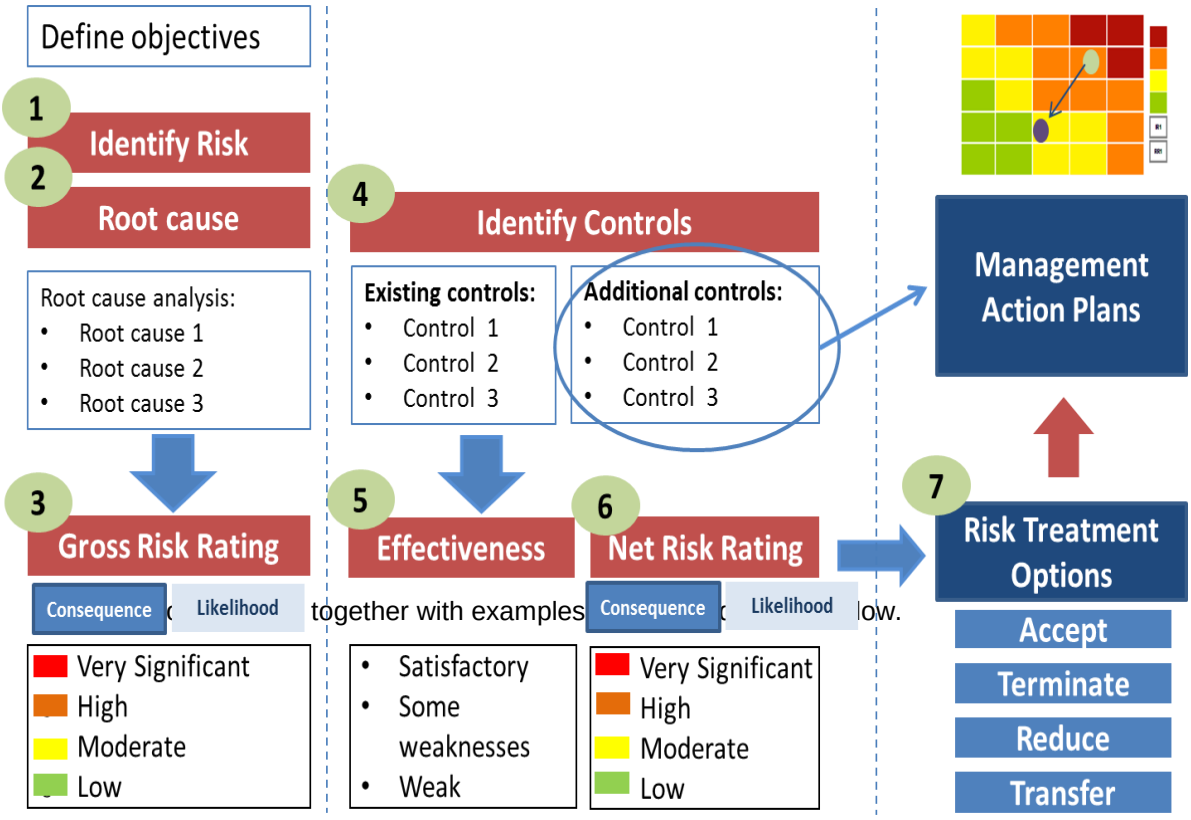
4. Risk assessment process

4.1 Overview

The diagram below depicts an overview of the risk management process in the ERM framework.



The risk assessment process is illustrated in the following diagram. The risk assessment technique employed is of scenario analysis technique, a most commonly used risk assessment techniques in the industry. This technique evaluates risks based on the possible risk scenario that potentially could occur and impact the objectives of an entity. On need basis, the CRO could direct other risk assessment techniques that are appropriate to risk assessment in Sunway, including techniques such as stress testing and value at risk.



4.2 Preparation

4.2.1 Define processes/activities/objectives

It is useful in the risk identification phase to have some assurance that all the key risks have been raised. The approach achieves this by first identifying the key processes and activities and objectives of each business unit.

The information is then used as a guide or "map" in the workshop session and in the preparation by business unit management prior to the workshop in thinking about the key risks.

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

4.2.2 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. 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 Sunway's risk appetite, which is defined as the level of risk Sunway is prepared to accept to achieve its objectives. Sunway's risk appetite can be expressed in terms of how much variability of return (i.e. risk) Sunway is prepared to accept in order to achieve a desired level of result (i.e. return). The objective of this exercise is to determine how much risk Sunway is willing to undertake.

Further, reference will be made to the Company'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 that the Company can sustain in any one year before the Company would face going concern problems. In a group structure, the group's risk parameters (Tier 1) shall be applied consistently to the business units with adjustment on the magnitude of the value, which is sometimes call as Tier 2 risk parameters.

Taking the risk appetite and risk capacity into consideration, five (5) consequence categories are used:

Very Significant:	Extraordinary event / disaster with 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

The manner by which financial and non-financial parameters could be used to assess the financial impact of a risk event is illustrated in Appendix C.

Non-financial consequences (as mentioned in Appendix C) would also be addressed in the risk assessment process.

Participants would be asked to consider before the risk assessment workshop/ discussion, the risks which may threaten their operational area. For each of these risks, they are also asked to identify the potential causes and consequences of the risk event occurring.

4.3 Gross risk analysis

The risk assessment workshop/ discussion requires the participation of key managers in the business. It usually runs for two sessions (Session A for Gross Risk Analysis and B for Control assessment) of approximately 2 to 3 hours each and is facilitated by appropriate personnel from Group Risk Management. For effective results, both sessions can be conducted in the same day, for example Session A in the morning and Session B in the afternoon.

One-on-one interviews with management and/or staff may also be used where it is considered more appropriate than the workshop approach.

4.3.1 Step 1: Identify risks

Participants identify the key business risks associated with the processes within their business area. They also nominate the person or persons responsible for managing each risk area.

4.3.2 Step 2: Determine cause

Participants identify the situation(s) or cause(s) which could result in the risk event occurring. The main causes of the risk are then utilised to determine within which broad risk category the risk should be recorded.

Example:
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.

4.3.3 Step 3: Determine Gross Risk Rating

a) Gross Consequence

Participants are asked to describe the consequences associated with each risk.

Example:
The following consequences may be identified as flowing from the risk of the loss of key personnel: • recruitment costs; • production interruption; • training costs; • loss of morale; and/or • reputation damage.

A rating is then assigned to each risk based on the consequences described. Primarily, this rating will be determined by the financial rating (explained above). However, other non-financial consequences (e.g. delay in project progress, number of resignation and reputation damage) are also considered in determining the rating.

b) Gross likelihood

Participants are asked to assign a likelihood rating (i.e. how likely is it that the entity will be exposed to each risk?). Consideration is 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 usually used are presented below:

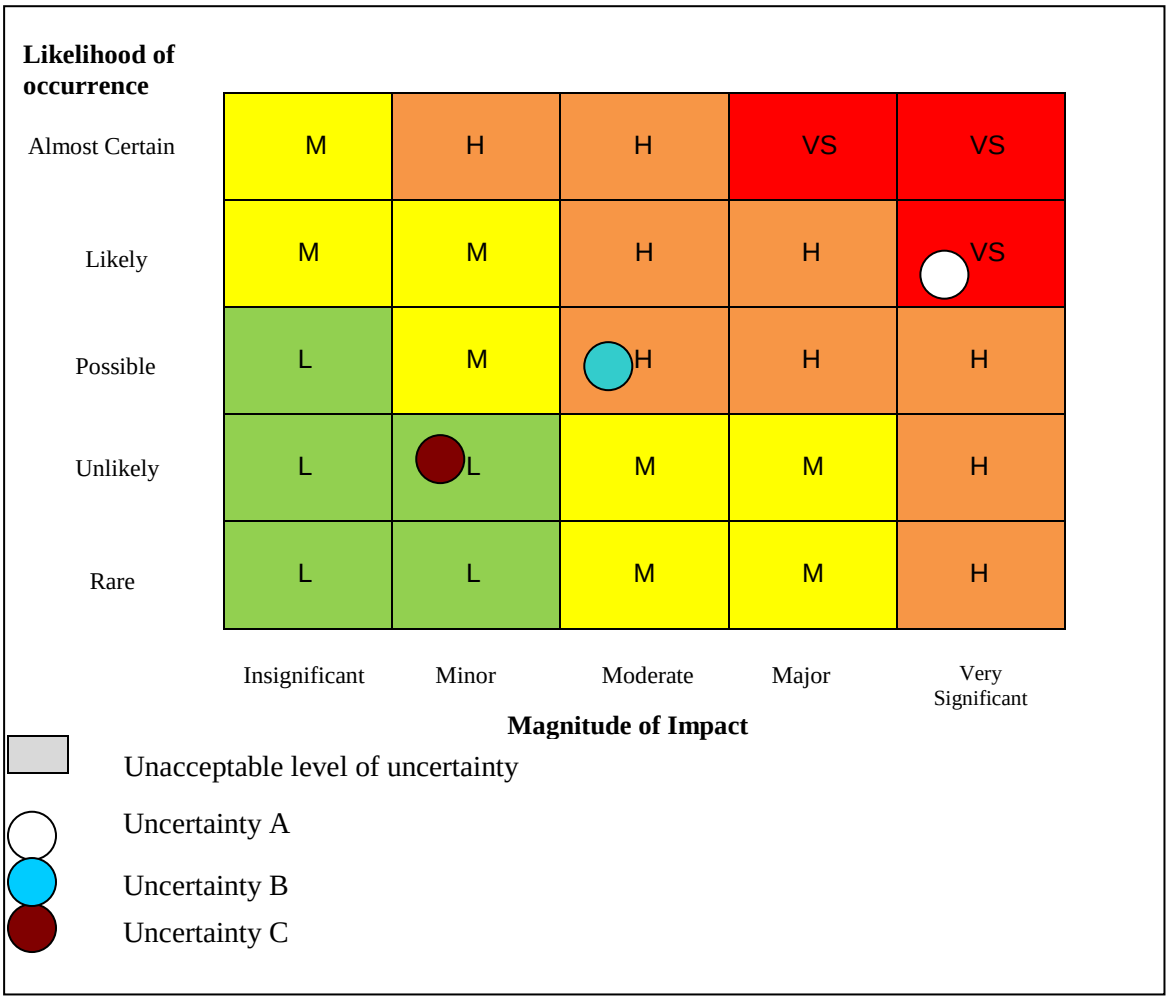
Description	Description
Almost Certain	The event is expected to occur in most circumstances, e.g. approximately above 95% chance of occurring in the next 12 months
Likely	The event will probably occur in most circumstances, e.g. approximately below 95% but above 50% chance of occurring in the next 12 months
Moderate	The event might occur at some time, e.g. approximately below 50% but above 25% chance of occurring in the next 12 months
Unlikely	The event could occur at some time, e.g. approximately below 25% but above 5% chance of occurring in the next 12 months
Rare	Event may occur only in exceptional circumstances, e.g. approximately below 5% chance of occurring in the next 12 months

Gross risk rating

The consequence and likelihood ratings identified are used to determine the gross risk rating for each risk. The table used is illustrated below:

	CONSEQUENCES/ IMPACT				
	Insignificant	**Minor**	**Moderate**	**Major**	**Very Significant**
LIKELIHOOD					
Almost Certain	Moderate	High	High	Very Significant	Very Significant
Likely	Moderate	Moderate	High	High	Very Significant
Moderate	Low	Moderate	High	High	High
Unlikely	Low	Low	Moderate	Moderate	High
Rare	Low	Low	Moderate	Moderate	High

The gross risk matrix can be illustrated as below:



By mapping the parameters for magnitude of impact of a risk against the likelihood parameters, the gross risk rating is determined using the risk matrix table as illustrated above. The most significant risks are in the top right hand area of the matrix (denoted by "VS" or "H" for Very Significant and High risk ratings respectively). These high gross risks

are determined before taking into consideration the control effectiveness to be completed in the Workshop - Session B. These are the important areas to Sunway and will be the focus of the workshop.

4.4 Control assessment (Pre-Work for Workshop – Session B)

4.4.1 Step 4: Identify controls

At the end of Session A in the workshop, the risks identified will be allocated between the responsible managers to enable identification of positive and negative controls in relation to the risks identified. The pre-work will be completed in group discussions before the commencement of Session B, which primarily focuses on control effectiveness assessments.

The information collected in Session A will be collated and provided in the following session. All managers will be provided with the *risk registers* for each risk for which they have identified as the responsible manager.

An example of the risk register is provided in Appendix D.

The managers are asked to review the Existing and additional controls considerations in determining the control effectiveness rating as follows:

Example:	
Risk of loss of key personnel:	
Existing controls	**Additional controls**
• awareness of market remuneration levels	• to implement succession planning
• regular remuneration reviews	• to establish career development program
• well developed training program	

Note: Additional controls could be selected for management action plan if considered appropriate.

4.4.2 Step 5: Determine control effectiveness

Once the key controls have been identified, an assessment of the effectiveness is made. Management or the participants perform self-assessment on the control effectiveness. Controls can be evaluated as Satisfactory, Some weaknesses or Weak.

Satisfactory	Controls are strong and operating properly, providing a reasonable assurance that the objectives are being achieved.
Some Weaknesses	Some control weaknesses / 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.

The effectiveness of the controls is assessed in terms of their design strength and the overall likelihood of effectiveness in reducing the gross risk to residual risk.

4.5 Conduct Workshop – Session B

4.5.1 Step 6: Challenge/Revise ratings

During the Workshop – Session B, the management team is given the opportunity to discuss and challenge the rating proposed as a result of the work undertaken prior to the workshop. Changes to ratings may result.

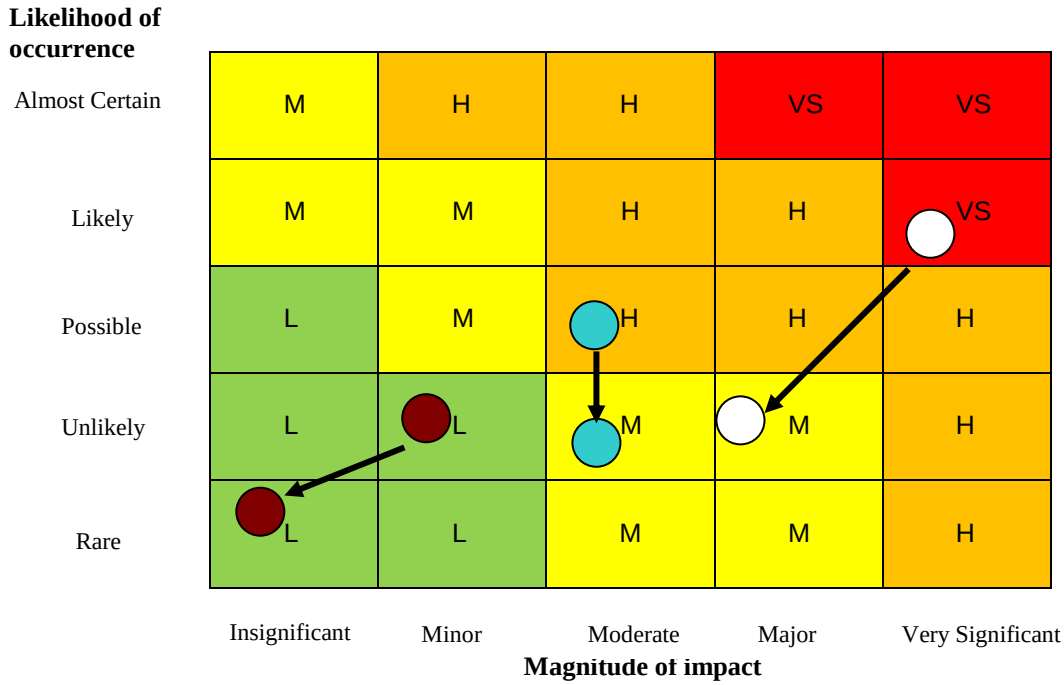
4.5.2 Determine current residual risk rating

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

This rating is a combination of the gross risk rating (Step 3) and the control effectiveness rating (Steps 4 and 5). For example, if the controls were satisfactory, the gross risks categorised as "Very Significant" (concentrated on the top right hand area of the risk matrix) would be moved downward towards the "Moderate" or "Low" areas of the matrix (bottom left hand area of the matrix).

The residual risk matrix below illustrates the movement of the gross risk to residual risk after taking into account the control effectiveness in place which mitigates the gross risks mentioned in step 5:

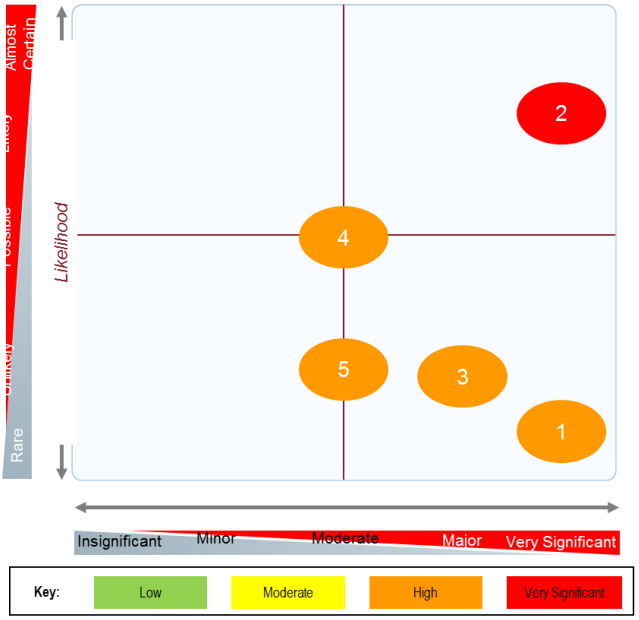
Residual risk matrix



4.5.3 Risk profiling

After the workshop, the risk registers and residual risk ratings will be confirmed by the management team. A risk profile will be prepared as illustrated in the chart below (illustrative example only):

No.	Risks		
1	Fire Outbreak	Combination – controllable/ uncontrollable	Discreet
2	Market glut	Combination – controllable/ uncontrollable	Discreet
3	Failure of essential equipment	Combination – controllable/ uncontrollable	Discreet
4	Economic downturn	Combination – controllable/ uncontrollable	Discreet
5	Human capital – Shortages	Combination – controllable/ uncontrollable	On-going



Key

C - Controllable (Management can prevent risk occurrence)

Comb - Combination of controllable and uncontrollable

UC - Uncontrollable (Management cannot prevent risk occurrence; it can only detect risk occurrence and manage risk consequence)

D - Discrete: One time event nature of risk that impacts operating earnings over a discrete time frame that may reoccur.

OG - Ongoing Risks: Iterative trend nature of risk. Economic, market, and regulatory conditions that impact operating earnings over an indefinite time frame.

At the completion of this risk assessment process, the management team then must consider the residual risk levels and decide whether they are acceptable in the context of the entity's objectives. The objective is not to eliminate all residual risk but rather to ensure that residual risk is maintained at an acceptable level in a cost effective manner.

4.5.4 Step 7 – Risk treatment options

The risk profile enables the management team to make conscious and visible risk management decisions. The options available to management teams in addressing residual risk, which is at an unacceptable level after a risk profile has been completed, are discussed in detail in Section 6. Risk treatment options: Accept, Terminate Reduce or Transfer risk.

4.4.5 Carry out self-assessment

Self-assessment promotes the philosophy that it is the people who work in the area who should be involved in the planning, implementing and monitoring of the controls in their area of responsibility. Management may decide that it is appropriate for people in their area to more closely assess their controls. Self-assessment can be carried out in a workshop situation, or by comparing existing controls against benchmark guides.

4.5.6 Internal audit

The risk profile also enables an effective internal audit plan to be developed as:

- the risk profiles will provide the internal audit department with a framework to prioritise operational reviews throughout the Group;
- management and personnel can be directed to high risks on an informed basis; and
- an overall audit plan can be developed in the risk assessment process.

4.5.7 Report to stakeholders

The reporting of the status of risk and control within the Group needs to be simple and employ visual dialogue concepts to convey the information.

The overall intention of the reporting process is to eliminate duplication at all levels and to provide a system that can cross divisional and product boundaries, thereby facilitating a broad benchmarking and comparative analysis base.

5. Risk communication

5.1 General concepts

Communication and consultation are an important consideration at each step of the risk management process. It is important to develop a communication plan for both internal and external stakeholders at the earliest stage of the process. The factors to consider in addressing the issues relating to both the risk and the process to manage the risk are:

- communication and consultation should involve a two-way dialogue between stakeholders with efforts focused on consultation rather than a one-way flow of information from decision maker to other stakeholders;
- internal communication should be centrally collated, either by the Risk Management Committee or the appointed Chief Risk Officer, with input directly from the business units/ functions at the point of identification;
- periodic management summary should be prepared (see Sections 5.2 and 6.2) and defined exceptional reporting should be established; and
- since stakeholders (internal and external) can have a significant impact on the decisions made, it is important that their perceptions of risk, as well as their perceptions of benefits, be identified and documented and the underlying reasons for them understood and addressed.

The next sections detail the risk communication processes.

5.2 Nature and timing of reporting

The following table illustrates the timing and frequency of reporting of each of the reporting units:

Departments/ Functions	**Reporting to**	**Frequency of reporting**	**Report/ Format**
Holding Company level			
Risk Management Committee ("RMC")	Board of Directors	Every quarterly	• Summary of key risks • Group risk profile* • Risk dashboard reporting – action plan status* • Flash report on new emerging risks, on need basis.
Group support functions	Sunway Exco	Regular standard reporting** (operational and financial)	• Standard reports
Business unit level			
Risk Working Committee ("RWC")	RMC	Every quarterly	• Summary of key risks • Business unit risk profile*

Departments/ Functions	Reporting to	Frequency of reporting	Report/ Format
			• Risk dashboard reporting – action plan* • Risk registers for critical risks • Flash report on new emerging risks (on need basis)
Business unit support functions	Head of Business Unit	Regular standard reporting** (operational and financial)	• Standard reports
Other Assurance			
Internal audit	Audit Committee	Based on internal audit plan	• Internal audit reports**

** Top 5 risks, or all critical risks, as necessary*

*** Not covered in this document, but may include such reports as management reports, budget variance analyses, etc.*

6. Risk action plan and monitoring

6.1 Formulating risk treatment plans

6.1.1 Prioritisation of risk

Management should identify and agree on the key risks which should be addressed first. Using the risk profile, choose the risks to be addressed first. There are various ways and considerations in which Management may choose/ consider to prioritise the risk – for example:

Example 1 – Prioritising risk in accordance with the rating attached to it, i.e. Very Significant, High, Moderate or Low.

Example 2 – Prioritising risk based on:

- risks that may cause high impact losses, even if such occurrences are infrequent;
- high frequency but low impact losses that can drain financial resources due to their cumulative effect;
- risks for which there is an obvious, practical and cost-effective solution that can be easily implemented; and
- risks that threaten the entity's public image and reputation.

Example 3 – Prioritising risk based on its impact to Sunway.

Management should create a preliminary risk map of the entity's risk exposures and the potential effect of risk on the entity's resources. Each cell of the risk map represents the effect a particular risk may have on essential/ scarce resources. These essential resources will be matched against the risk parameters set in Section 4 and finally to the identified risk.

- Management should be able to make a decision based on the risk map and direct its attention to those risks that may inflict greatest harm (by reference to essential resources);
- The level of importance placed on these resources varies from one organisation to another. Some of the factors to consider include the size of the company, e.g. a public listed company like Sunway would generally place more importance on its image and reputation compared to its financial resources whereas a smaller organisation would place more priority on financial resources. All these depend very much on the strategic direction and objectives of that organisation; and
- With the risk priorities in hand, the Management can now gather to review the results and create a comprehensive action plan to address high-priority risks. Other risks would not be agreed totally but, your attention should be directed first to those risks that threaten greater harm.

6.1.2 Action task

Upon determining the priorities in risk treatment, the following tasks would have to be put in place:

Task	Focus
Action plan	Determine the plan to be undertaken to manage the risk based on the risk treatment

Action cost	Ascertain the estimated cost for risk treatment.
Expectations/ benefit	Ascertain the expected outcome to be generated from the planned action, e.g. in monetary terms (cost savings/ revenue generation) or KPIs (debtors days to be reduced from 90 days to 60 days)
Risk owner	A named person responsible for the action: it is important to identify a named person for leading or coordinating the action. Most individuals and teams will need to take some responsibility for risk management issues, but this will depend on their skills and time available.
Completion date	Time scale for action: this may depend on the nature of the problem and action required, short term actions can be deployed almost immediately; medium term action normally require a longer time, perhaps up to 6 months to implement. Long-term actions are those that will take more than 6 months to be implemented.
Action status	Status of the action plan.

The action tasks should also be aligned with the management action plan.

Risk treatment options:
There are four (4) core response strategies to the management of residual risk:

Accept
Risks may be accepted with full intent and purpose and you can make a conscious decision not to take any action.

Reduce
You can accept the risk but take some actions to lessen its likelihood or impact such as through organisational procedures (e.g. segregation of functions), guidelines, internal monitoring system and internal auditing.
Risk monitoring includes evaluating the effectiveness of the risk treatment plan, review risk strategies and the risk management system which is set up to control implementation. Risks and the effectiveness of control measures need to be monitored to ensure changing circumstances do not alter risk priorities.
Ongoing review is essential to ensure that the management plan remains relevant. Factors which may affect the likelihood and consequences of an outcome may change, as may the factors which affect the suitability or cost of the various treatment options. It is therefore necessary to regularly repeat the risk management cycle. Review is an integral part of the risk management treatment plan.

Pass on
Management can choose to pass on all or part of a certain risk to other parties such as insurance contracts and other agreements permit shifting of risks to a counter party (e.g. insurance against certain perils).

Terminate
Risks may be eliminated by not engaging in the activities/ function with the attendant risks.

Refer to Appendix A for further explanation on the 4 options mentioned above.

Action cost
Prior to implementation of a risk action the relevant action, cost must be agreed with the budget owner, taking into account the cost/ benefit of the action. Secondary risks, which may occur as a consequence of the primary reduction action, should also be considered.

Expectations/ benefit
Once the action plan has been agreed upon, risk owner must identify and state the expectation or benefit that is to be achieved from the plan, i.e. financial and/ or non-financial.

This expectation/ benefit would then be used as a benchmark by Management to check the action status upon completion of the action plan on the agreed completion date.

Risk owner
Next you have to identify a named person responsible for the action: it is important to identify a named person for leading or coordinating the action. Most individuals and teams will need to take some responsibility for risk management issues but, this will depend on their skills and time available.

Generally, the risk owner will be the team leader leading the formation and execution of the plan whereas the rest of the team members will be responsible for assisting in executing the plan. The team members selected to manage the risk could be from other departments or within the department in which the risk resides.

The risk map can guides you on where the risk resides (i.e. which department is affected by the risk) for all the risks identified. This risk map would guide the risk team in formulating its team members to address the risk. The formation of the team is based on the following principles - the risk team should:

- be small enough to function efficiently;
- include enough members to carry out team activities;
- include members who are reliable and committed to the success of the risk team, and who have access to research resources and the necessary skills and expertise;
- include people knowledgeable about the Group and the operations included in the scope of the project-team members need not be risk experts; and
- use committees of non-team members to provide needed expertise without making the team too large.

Completion date
A management action plan with a realistic completion date for each risk action should be determined and recorded. There may be several risk actions to reduce the consequences or likelihood of the risk occurring. If the risk actions relate to a key risk on the initial assessment, the actions are to be identified as key actions as part of the risk treatment process.

The impact of risk actions on the achievement of objective must be planned and agreed. The risk treatment may involve the use of a control measure (a process to be used to treat a common risk).

Action status
The status of action plan should also be disclosed to enable the relevant parties to assess the status and also the progress of risk action plan.

6.1.3 Complete and circulate the action plan

- Document the chosen strategies onto a risk action plan endorsed by the Team leader and Team members;
- Obtain endorsement/ sign-off of the plan by upper Management – Head of Department/ CEO/ AC/ BOD, where applicable;
- Share appropriate sections of the plan with department heads, departmental safety/risk committees and other employees whose activities the plan affects;
- Prepare general information about the action plan for dissemination to the general employee population; and
- The AC and Risk Coordinator are responsible for following up on decisions made by the respective parties and communicating the decisions to the respective parties in order to ensure a smooth flow and communication loop is maintained for strategies on risk action plan.

6.1.4 Reviewing and updating of risk profile and risk mitigation plans

Reviewing and updating
The CRO or Risk Coordinator and risk owners are responsible for monitoring, reviewing, updating and documenting the following reports on a quarterly basis or as and when the need arises.

The following report would be required for monitoring, reviewing, documenting and reporting as follows:

Task	Focus
Risk parameter	• The parameters used to estimate the consequences of a risk should it occur will be based on Sunway's risk appetite; • There should not be any changes made to the risk parameters once they are set for the year unless there is a significant shift in the risk appetite of the Management (what constitutes a significant shift is subject to discretion of Management); and • As risk appetite is subjective in nature and influenced by various internal and external factors, the risk parameters have to be reviewed at least on a yearly basis to ensure changes in circumstances/ risk appetite are fairly reflected in the risk parameters.
Risk register	Risk analysis – involving the risk identification, control assessment and measurement. Information required to be updated includes: • all details in the report involving the relevancy of the description, causes, consequences, controls and measurement. Changes to the above information could be influenced by factors such as:

Task	Focus
	- changes/ revisions made to risk parameters due to changes in strategies, objectives and direction of the Group or the internal operating environment within the Group (changes in risk appetite); - the macroeconomic factors; and - successful execution of the risk treatment plan of existing risks. ● Whilst updating the risk profile, be vigilant for any correlation of risks that may arise such as: - positive correlation with other risks, i.e. as the likelihood of one risk increases, the likelihood of an associated risk may also increase. This means that the impact of a risk may be accompanied by additional effects that could catch you by surprise if you fail to recognize these correlated risks. At the same time, it may mean that steps taken to mitigate one risk also could positively impact another risk; and - negative correlation of risk. This means that as the likelihood or impact of a risk increases, that of an associated risk may decrease and vice-versa.
Risk action report	The risk action report has to be reviewed and updated. This includes evaluating the effectiveness of risk treatment plan and risk strategies. This involves assessing and updating the status of risk treatment plans and whether the risk treatment plan is achieving its objectives by reference to: ● the KPIs relating to success of the risk treatment; and ● whether the additional controls deployed are addressing the core issue of the risk. The above requires regular review, e.g. factors which may affect the likelihood and consequences of an outcome may change, as may the factors which affect the suitability or cost of the various treatment options. It is therefore necessary to regularly repeat Risk Management cycle and ensure the necessary information is updated accordingly.

The above reviewing and updating has to be coordinated by the respective Risk Coordinator with the relevant process owner/ HOD/ risk owner. There are many ways in which risk monitoring and review could be performed, for example:

- interview sessions;
- workshop sessions; and
- group discussions.

The CRO would have to communicate the above information to RMC via e-mail on changes made to the above information/ reports.

6.2 Key monitoring functions

6.2.1 Management functions

Risk management supervision is the managerial duty of the respective supervisor which cannot be delegated. Some of the procedures are firmly incorporated in the internal control procedures of the Group. Examples of tools that are being used are:

- monthly budget variance analysis;

- monitoring for compliance with reporting threshold, e.g. Bursa announcements, accounting standards compliance, etc;
- regular analysis of intragroup information and external information on market data, changes in regulations, etc;
- human resource management especially on personnel recruitment, retention, appraisal and succession planning; and
- staff training and skill development.

6.2.2 Internal audit function

Internal auditors should play an active role, which focuses on:

- facilitating systematic profiling of all risks of the Group;
- providing objective assurance on the adequacy and integrity of the existing system of internal control, including the ERM processes; and
- continuous application of the ERM policies and procedures as set out in this document.

6.2.3 External auditors

External auditors conduct a systems audit of the risk management that focuses on:

- systematic approach to risk management;
- adequate communication of risk management issues / risk policy principles; and
- sample-testing of risk management for effectiveness and continuous application, all with a view of expressing an opinion on the financial statements.

Through such a systems audit, the statutory auditors ascertain whether the steps taken by the auditee are generally appropriate to identify, assess and communicate the significant risks so that management can properly respond.

6.3 Documentation

Each stage of the risk management process should be documented. Documentation should include assumptions, methods, data sources and results.

The documents used are:

- risk register;
- executive summary;
- risk profile/ matrix;
- risk dashboard reporting; and
- flash report (see below).

As an exception to the regular risk reporting set out in Section 4, ad-hoc reporting through flash report relates to sudden and unexpected risks impacting significantly on the Group's net assets, financial position or results of operations. These are reported directly to the RMC for onward reporting to the Board of Directors, without following the usual reporting channels. The same applies to events and incidents already occurred or expected if involving reputation risks, significant safety, health and environment issues or major financial losses. The ad-hoc or flash reporting mechanism aims to immediately inform the Management Committee and the Board about sudden significant risks or pertinent risk issues.

7. Integration of ERM

The business environment is constantly changing and as a consequence implementing ERM is a never ending process. Sustaining ERM requires constant attention by the Senior Management, and integration into on-going management initiatives sends a message to staff at all levels of its importance. Some of the opportunities for integrating ERM in on-going management activities include:

- corporate governance;
- strategic planning; and
- Balanced Scorecard ("BSC").

Sunway Group should develop a structured training programme and yearly ERM communication plan throughout the business units, which should incorporate ERM refresher courses to the risk coordinators. The training sessions would need to address elements of the above mentioned activities to ensure effective integration of ERM across the Group.

In today's risky world, organisations can no longer rely on a silo approach to risk management but need an integrated and holistic perspective of all the risks facing the organisation. A risk-centric organisation does not avoid risks but rather knowingly takes risks aligned with its risk appetite. Integration of ERM with ongoing management activities serves to embed risk management throughout the Group.

7.1 ERM and Corporate Governance

ERM ties in closely with corporate governance by:

- improving information flows between the company and the Board regarding risks;
- enhancing discussions of strategy and the related risks between executives and the Board;
- monitoring key risks by accountants and management with reports to the Board;
- identifying acceptable levels of risks to be taken and assumed;
- focusing management on the risks identified;
- improving disclosures to stakeholders about risks taken and risks yet to be managed;
- reassuring the Board that management no longer manages risk in silos; and
- knowing which of the organisation's objectives are at greatest risk.

7.2 ERM and Strategic Planning

ERM and strategy setting should be viewed as complimenting each other and not as independent activities. If strategy is formulated without identifying the risks embedded in the strategy and assessing and managing those risks, the strategy is incomplete and at risk of failing. Similarly, if ERM does not begin with identifying risks related to the Group's strategy, the effort will be incomplete by failing to identify some very important risks.

Strategy formulation is enhanced by ERM because risks are identified, and the strategic alternatives are assessed given the Group's risk appetite. In turn, without a well articulated strategy, the foundation for implementing ERM is insufficient. Viewing the two together forms the basis for a strategy-risk-focused organisation.

7.3 ERM and BSC

The BSC is a tool for communicating and cascading the Group's strategy throughout the organisation. Sunway's BSC captures the Group's strategy in four key perspectives:

- financial;

- customer;
- internal process; and
- learning and growth.

Integration of the BSC with ERM can enhance performance management. In the BSC, objectives are identified for each of the perspectives, and as noted previously, ERM begins with an understanding of objectives. For each BSC perspective, metrics (key performance indicators—KPI's) are selected and stretch targets are set. ERM adds value to the BSC through the identification of events (risks) that could stand in the way of achieving the targets in each of the four perspectives. By monitoring the KPI's, management can assess how effectively their risk mitigation efforts are working. In effect, the KPI's for each perspective also serve as key risk indicators (KRI's) although they are not initially selected for that purpose. For example, if a target for customer satisfaction is not achieved, it suggests that some risks related to the item exist. The same metric can be used for monitoring both strategy and risk. Thus, risk parameters used to measure risks, as shown in Appendix C, should be based on the strategic objectives and KPIs, reflecting the risk appetite of the Group.

The BSC can be integrated with ERM to manage and monitor risk related to the strategic objectives. Using a risk dashboard for the key risks identified in each of BSC perspectives is a way to assign responsibility for managing the risk.

The focus area identifies the risks as strategic, operational, or financial. Management's self-assessment of its risk mitigation actions is shown in the worksheet by asking: "Is it in place? If so, how effective is it?" The risk dashboard also focuses on identifying the owner of the risk who will be held accountable for managing it. A risk dashboard, if maintained on Sunway's intranet, allows management to review the dashboard at any time, which adds strength to the accountability for the management of the risk.

8. Conclusion

A risk management document advances a more systematic and integrated approach for risk management. By focusing on the importance of risk communication and risk tolerance, it looks outside the organisation for the views of the public. Internally, it emphasises the importance of people and leadership and the need for departments and agencies to more clearly define their roles. The framework provides a tool that helps organisations communicate a vision and objectives for risk management.

Risk management can become a strategic competitive advantage if it is used to identify specific action steps that enhance performance and optimise risk. It can also influence business strategy by identifying potential adjustments related to previously unidentified opportunities and risks. Used appropriately, risk management thus becomes a means of helping the organisation shift its focus from crisis response and compliance to evaluating risks in business strategies proactively, to enhancing investment decision-making and to improving shareholder value. Organisations that develop an enterprise risk management framework for linking critical risks with business strategies can become highly formidable competitors in the quest to add value for shareholders.