LONGHORN PUBLISHERS LIMITED

RISK MANAGEMENT FRAMEWORK POLICY & PROCEDURES MANUAL

CONTENTS

1. RISK MANAGEMENT POLICY

1.0 Overview

The Longhorn Publishers Limited (LPL) Risk Management Framework is a reference document that provides information on the risk management framework within which LPL's risks are managed. The framework is considered to be dynamic as it evolves over time to incorporate developments in tools and practices in the area of risk management.

The prudent management of risks is a key element of achieving LPL's strategic objectives. In this regard, LPL manages its activities according to a set of key principles. To the extent possible, LPL takes thorough steps to limit or mitigate the risks that arise in the course of its operations. The main risks that LPL strives to mitigate include credit, market, liquidity, legal, Information Technology and operational risks.

The risk management framework seeks to align business opportunities and the taking of risks to the ever present challenges of the company in achieving its mission and core objectives. It encompasses the whole spectrum of risk ranging from the high level enterprise-wide strategic business risks to individual departmental/section operational risks.

Guiding Principles

- Independence: Risk monitoring and oversight, supported by analytic capacity and a governance framework which is independent of management operations.
- Risk Culture: The Audit & Risk Department strives to create a culture where risk management is highly valued, considered an integral part of all management activities, and viewed as the responsibility of all staff.
- Risk Identification: All existing and new lines of business are thoroughly reviewed on an ongoing basis to identify all relevant risks.
- Risk Mitigation: Credit, market, liquidity, legal, Informational Technology and operational risks are mitigated to the extent possible.
- Risk Measurement: Appropriate quantitative and qualitative measures have been developed in line with policies and guidelines.
- Monitoring and Reporting: Reports provide context and significance to managers on issues surrounding risk management and the company's overall risk position and are prepared on a regular basis.
- Review: Periodic review of risk management policies, procedures and operations are undertaken.

1.2 Objectives

The main objective of the LPL's Risk Management Policy is to ensure the implementation of an effective risk management framework that is consistent with the company achieving its policy and operating objectives.
The principle underpinning the company's approach is that risk management is an integral part of the management function in the organization. Line managers have the responsibility to evaluate their risk environment, to put in place appropriate controls and to monitor the

effectiveness of these controls. This process is supplemented with a review of key enterprise risks by the Audit & Risk Committee.

LPL is committed to ensuring that effective risk management remains central to all its activities and is a core management competency. This framework has been developed to:

- Allow the company to proactively manage its risks in a systematic and structured way and to continually refine its processes to reduce the company's risk profile thereby maintaining a safer environment for all its stakeholders;

- Ensure appropriate strategies are in place to mitigate risks and maximize opportunities;

- Embed the risk management process and ensure it is an integral part of the company's planning process at a strategic and operational level;

- Help create a risk awareness culture from a strategic, operational, individual project perspective;
- Give credibility to the process and engage management's attention to the treatment, monitoring, reporting and review of identified risks as well as considering new and emerging risks on a continuous basis;
- Recognize the need for, and align, the holistic enterprise-wide "top down" strategic assessment with the "bottom-up" operational and strategic risk assessment.

1.3 Policy Statement

1. The Board of Directors, and the Audit & Risk Committee, have responsibility for the oversight of risk management framework within Longhorn. The Board will determine that appropriate risk management strategies and policies are in place, and that these processes are adequate and effective.
2. The Board has assigned responsibility for risk management to the Risk Management function that is domiciled in the Audit & Risk department. The Chief Audit & Risk Officer has a direct reporting line to the Board Audit & Risk Committee. The objective of this reporting line is to ensure that, if required, there is the possibility for an independent reporting to the Board in respect of the organization's risk profile.
3. The Audit & Risk function will aid in the identification, assessment, prioritization and formulation of appropriate responses to the risks facing the company. The risk management processes will be required to ensure that:
    a. Risks arising from business strategies and activities are identified and prioritized.
    b. The Board and Management have determined the level of risks acceptable to Longhorn including the acceptance of risks designed to accomplish the company's strategic plans.
    c. Risk management activities are designed and implemented to reduce, or otherwise manage, risks that are determined to be acceptable to Management and the Board.

    d. Ongoing monitoring activities are conducted to periodically re-assess risk and the effectiveness of controls to manage risk.
    e. The Board receives periodic reports of the results of the risk management processes.

4. The Risk Management function will aid the Management in implementing a risk identification, assessment, and management process comprising:

   a) Identifying, assessing and prioritizing the current and future vulnerabilities in the short, medium and longer-term.
   b) Quantifying the potential exposures / vulnerabilities in terms of:
      - Likelihood of occurrence;
      - Impact in the event of crystallization

   c) Designing and implementing appropriate procedures and operational guidelines to respond / mitigate each risk to the degree required. The range of responses to the identified risks may include:
- Designing appropriate controls to mitigate the identified risks;
- Transferring risks to 3rd parties via, say, insurance;
- Disengaging from the activities that may be considered to be inordinately risky;
- Choosing to 'carry' any element of residue risk that cannot be eliminated / controlled by any of the three methods above.

   d) Implementing cost-effective controls and assigning responsibilities for overseeing implementation of controls. Ideally, each major risk area should have an identified 'risk owner' responsible for managing and monitoring the identified risks for his / her area.

   e) Monitoring the effectiveness of controls instituted to mitigate identified risks. The Board and Management review operating results, etc, to assess whether the current policies and procedures are having the desired outcome and whether the company is adequately managing risk. Monitoring may be weekly, monthly or less frequent depending on the likelihood / impact of vulnerability.

   f) Determining whether, arising from the oversight and evaluation process, there is need to revise the risk management strategies, policies and procedures to address new risks or enhance control measures.

2. ROLES AND RESPONSIBILITIES

The board, management and all employees have role to play in ensuring that business risk is effectively managed across the organization. The risk management framework has been fully endorsed and supported by the Board of Directors who set the organizational tone for risk management and champion the benefits through all levels of the business. This document formalizes those inherent responsibilities to manage risk which are as below:

2.1 Role of the Board

The board will provide oversight with regard to the risk management framework by:

- Knowing the extent to which management has established effective enterprise risk management in the organization.
- Being aware of and concurring with the entity's risk appetite.
- Reviewing the entity's portfolio view of risk and considering it against the entity's risk appetite.

- Being appraised of the most significant risks and whether management is responding appropriately.
- Provide comment and challenge on risk management activity and progress.

2.2 Role of the Management Committee

The role of the Management Committee will include the following:

- Oversee the risk management process of the company as a whole, on behalf of the Board.
- Identify and assess fundamental risks affecting the company, and ensure that arrangements are in place to manage those risks.
- Co-ordinate the various functional activities which advise on risk management issues within the organization.
- Regularly review and recommend to the Board the organization's risk appetite or level of exposure for the company.
- Identify and consider major decisions affecting the company's risk profile or exposure.
- Embed a risk management culture within the organization, through appropriate risk education, high level controls and procedures.
- Applying a risk management focus in making business decisions

2.3 Role of the Audit & Risk function

The role of the Audit & Risk function will include the following:

- Facilitate and monitor the implementation of effective risk management practices by operational management and assists risk owners in defining the target risk exposure and reporting adequate risk-related information throughout the organization.
- Prepare reports on organizational risks for the board and other stakeholders.

- Focus internal audit work on the significant risks, as identified by Management and auditing the risk management processes across the organization.
- Provide assurance on the management of risk within the organization by carrying out risk based process audits.
- Identifying known and emerging issues.
- Identifying shifts in the organization's implicit risk appetite.
- Provide active support and involvement in the risk management process.
- Facilitate risk identification/assessment and educating staff in risk management and internal control.
- Co-ordinate risk reporting to the Audit & Risk Committee.

- Review and update the Risk Management Framework - Policy and Procedure Manual.

2.4 Role of Employees

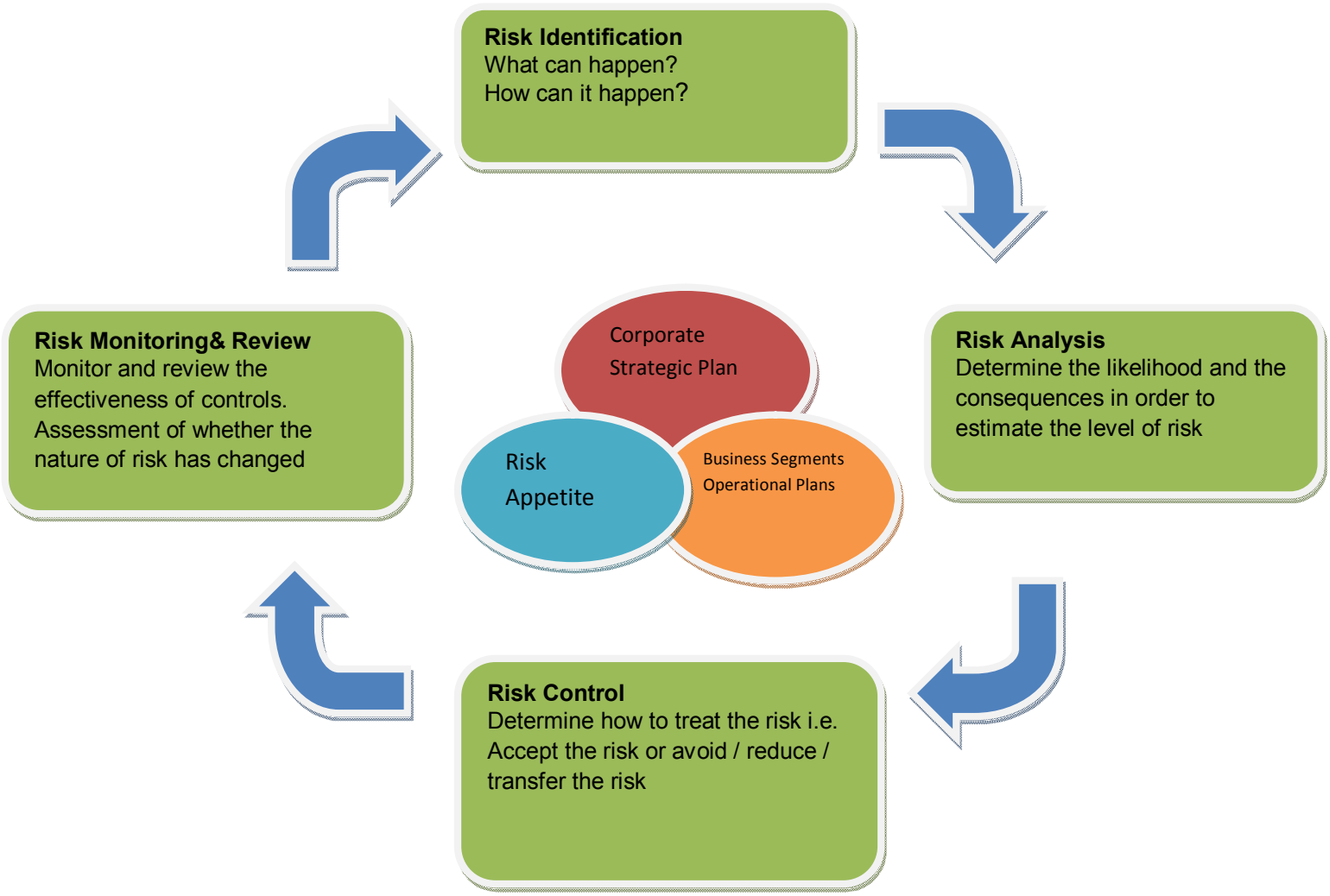
All employees are responsible for adhering to processes and procedures which are designed to manage risks associated with the work they perform. They are also required to alert management to any risk incidents or potential risk incidents that they become aware of in the course of their work. Employees should also discuss with their management any potential gaps in, or improvements to, the control framework that they identify.

3.0 RISK MANAGEMENT METHODOLOGY

3.1 Risk Management Cycle

LPL's risk management cycle

Risk management is composed of 4 key stages, as illustrated in the diagram below. For LPL the context of the exercise mainly revolves around the strategic plan of the organization, the plans of the specific business units and the risk appetite of the organization.



3.2 Definitions

Risk is defined as events that may prevent achievement of the aims or goals of the organization.
Risk Management is a systematic way of protecting business resources and income against losses so that the objectives of the organization can be achieved without unnecessary interruption.
Risk Assessment is the systematic process of identifying and prioritizing/analyzing risks.

3.3 Risk Assessment

Risk assessment involves Identifying and prioritizing issues, conflicts and other matters regarding the company's operations that may hinder the attainment of business objectives. This process requires the company to consider carefully its vulnerabilities.

a) Risk Identification

Risk Identification involves the collection all possible risks to the organization in a timely and proactive manner. Approaches used to identify risks include:-

- Use risks already identified in the risk registers, strategic plans, operational plans, and other key company source documents;
- Checklists, surveys, questionnaires;
- Team based brainstorming, structured interviews, focus groups, personal experiences;
- Facilitated workshops;
- Flow charting, systems analysis;
- Experience, local and overseas knowledge;
- Records, databases, insurance claims;
- Past organizational experiences;
- Internal and external reports/audits;

LPL will manage risks at three levels – corporate, department and projects as follows:

Corporate
Risks at the corporate level are those which would have a serious and potentially devastating impact on how we operate. Corporate risks tend to be those that would be noticeable by the public and would generate significant media coverage in the event of the risk occurring. Corporate risks normally impact across the range of our risk impact criteria (especially reputation) and can include strategy level risks in terms of decisions made about which direction the organization should be following. Controls for corporate risks will normally be cross-cutting and will be split across a number of departments or business areas. Risk ownership is required at the highest level (Board of Directors ,Group Managing Director, Executive Management) in order provide the appropriate leadership, scrutiny and management of the risk.

Department
Risks at the departmental level are those which would have a potentially serious impact for the department concerned, however the end result of these risks would not necessarily impact the organization overall. They may still be noticeable by other departments and could affect other areas of work, especially where departments are jointly delivering an initiative, however the biggest impact of the risk would be felt within the relevant department. Controls for departmental risks will, in the majority, sit within the department affected, however a few significant controls may still be situated in other business areas. Risk ownership at this level is normally assigned to the Head of Department; however some specific risks may be assigned to other senior officers especially in specialist subject areas.

Project
Project risk management follows the same principles as those defined in this document and uses the same risk assessment matrix to evaluate project risks. In most cases project risks remain within the project and are assigned to a designated member of the project team, but can also be escalated to either the departmental or the corporate level via the project sponsor who is responsible for the aggregated project risk.

b) Risk Prioritization/Analysis

Risk Prioritization involves the measurement or scoring of identified risks and the categorizing of risks as to their relative severity and potential impact to the organization.

Risks will be measured or scored according to;

- The Consequence (also called impact or significance) when a risk occurs. For example loss of cash, opportunity cost, tarnished company reputation etc.
- The Likelihood (also called probability) of the risk occurring.
- Likelihood and impact scores are commonly measured on a scale of 1 to 5.
- A measure of total risk will be ascertained by multiplying the two scores together.

The tables below illustrate the assessment criteria to be used in ranking organizational risks according to their impact and likelihood of occurring.

Risk Consequence Scale

Level	Descriptor	Business Impact Description
5	Catastrophic	To close down the organization, or a significant part, for a very long period
4	Significant	To prevent the organization achieving a major part of its objectives for a long time
3	Moderate	To stop the organization achieving some of its objectives for a limited period
2	Minor	To cause inconvenience but not affecting the achievement of significant objectives
1	Insignificant	To cause very minor inconvenience, not affecting the achievement of objectives

Risk Likelihood Scale

Level	Descriptor	Business Likelihood Description
5	Almost Certain	The future event(s) will more or less happen.
4	Probable	The future event(s) are expected to occur in most circumstances.
3	Possible	The chance of the future event(s) is more than unlikely but less than probable.
2	Unlikely	The future event(s) are less likely to occur/happen.
1	Rare	The future event(s) may occur only in exceptional circumstances.

Risks will be scored before and after taking account of the internal controls which manage the risks.

Inherent (or gross or absolute) risk scores will be measured by assessing the consequence and likelihood of a risk occurring before any internal controls are taken into account. Inherent risk scores will be used by internal auditors to prepare an audit plan that will provide assurance that internal controls are operating effectively.

Residual (or net or controlled) risk scores will be measured by assessing the consequence and likelihood of a risk occurring after any internal controls are taken into account. Residual risk scores will be used by management to formulate appropriate risk responses (internal controls) to mitigate the identified risks.

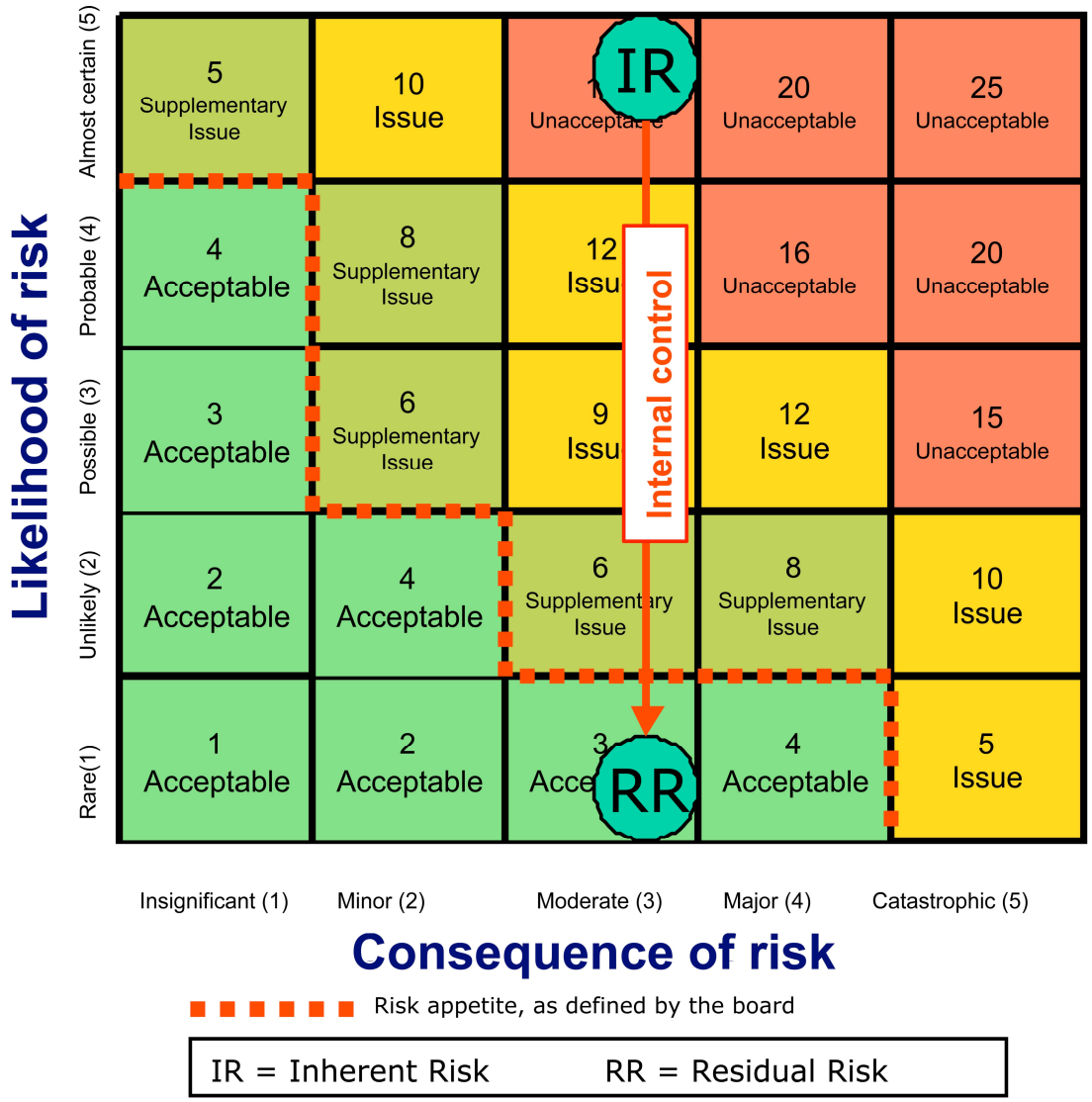
3.4 Risk Appetite

Risk appetite is the amount of risk exposure, or potential adverse impact from an event, that the organization is willing to accept/retain. Once the risk appetite threshold has been breached, risk management treatment and business controls will be implemented to bring the exposure level back within the accepted range.

LPL aims to be risk aware, but not overly risk averse and to actively manage business risks to protect and grow the organization. To deliver its corporate priorities, the organization recognizes that it will have to manage certain business risks.

Management will formulate and implement risk responses (Internal Controls) that will reduce the residual risk to within the organization's risk appetite. Internal Audit will conduct audits and provide assurance on whether management is managing organizational risks to within the risk appetite. The organization's risk appetite will be determined by the Audit & Risk committee with the assistance of the Management Committee.

LPL Inherent & Residual Risks rating and the Risk Appetite



Risk Rating	Type of issue	Risk Level	Guidelines for Risk Matrix
13 to 25	Unacceptable	(Ex) - Extreme	Eliminate, avoid, implement specific action plans / procedures to manage & monitor
9 to 12	Issue	(H) - High	Proactively manage
5 to 8	Supplementary Issue	(M) - Medium	Actively manage
1 to 4	Acceptable	(L) - Low	Monitor & manage as appropriate

3.5 Risk Responses

Risk responses fall within the following categories:

- Avoidance – Exiting the activities giving rise to risk. Risk avoidance may involve exiting a product line, declining expansion to a new geographical market, or selling a division.
- Reduction – Action is taken to reduce risk likelihood or impact, or both. This typically involves any of a myriad of everyday business decisions.
- Sharing – Reducing risk likelihood or impact by transferring or otherwise sharing a portion of the risk. Common techniques include purchasing insurance products or outsourcing an activity.
- Acceptance – No action is taken to affect risk likelihood or impact.

In determining risk response, management will consider such things as:

- Effects of potential responses on risk likelihood and impact – and which response options align with the entity's risk appetite.
- Costs versus benefits of potential responses.

Once management selects a response, it may need to develop an implementation plan to execute the response. A critical part of an implementation plan is establishing control/mitigating activities to ensure the risk response is carried out.

3.6 Monitor & Review

Monitoring of risks and treatment actions will be undertaken regularly to ensure risks remain within the tolerable level and that treatment actions have been implemented and are effective.

The review will include;

- an reassessment of the inherent risk based on changes in the internal and external environment;
- assessment of any emerging risks;
- assessment of the effectiveness and efficiency of the application of controls and new treatment actions

The Management Committee will continuously review the risks facing the organization and evaluate whether planned risk responses/mitigation actions have been implemented and have reduced the risk(s) rating to below the risk appetite.

3.7 The Risk Maturity Model (RMM)

Organizations wishing to implement a formal approach to risk management or to improve their existing approach need a framework against which to benchmark their current practice. Best practice benchmarks can be defined in terms of maturity, usually reflecting increasing levels of sophistication together with other features. The Risk Maturity Model (RMM) describes four levels of maturity, each linked to four attributes – culture, process, experience and application. LPL will use this model to assess its current level of maturity, identify realistic targets for improvement, and produce action plans for developing or enhancing its risk capability.

The RMM levels are as follows:

Level 1 - Risk Naïve

The Naïve risk organization is unaware of the need for management of risk, and has no structured approach to dealing with uncertainty. Management processes are repetitive and reactive, with little or no attempt to learn from the past or to prepare for future threats of uncertainties.

Level 2 - Risk Novice

The Novice risk organization is experimenting with application of risk management, usually through a small number of nominated individuals, but has no formal or structured generic processes in place. Although aware of the potential benefits of managing risk, the Novice organization has not effectively implemented risk processes and is not gaining the full benefits.

Level 3 - Risk Defined

The Defined risk organization has built management of risk into routine business processes and implements risk management on most or all projects. Generic risk processes are formalized and widespread, and the benefits are understood at all levels of the organization, although they may not be consistently achieved at all levels.

Level 4 - Risk Managed

The Managed risk organization has a risk-aware culture, with a proactive approach to risk management in all aspects of the business. Risk information is actively used to improve business processes and gain competitive advantage. Risk processes are used to manage opportunities as well as potential negative impacts.

Appendix Two provides the detailed attributes of culture, process, experience (people) and application (technology) on all the four levels of the RMM.

Appendix One: Risk Management Template

	Risk Identification			Risk Assessment							Risk Management	
				Inherent Risk Scores				Residual Risk Scores				
	Organizational Risk(s)	Risk(s) Implication	Company Process	Impact	Likelihood	Total Score	Current Internal Controls & Activities	Impact	Likelihood	Total Score	Risk Response & Mitigating Activities	Risk Owner & Implementation Date
1												
2												
3												
4												
5												
6												
7												
8												
9												
10												
11												
12												
13												
14												
15												
16												
17												
18												
19												
20												

Appendix Two: Attributes of RMM Levels

	Level 1 - Risk Naïve	Level 2 - Risk Novice	Level 3 - Risk Defined	Level 4 - Risk Managed
Definition	Unaware of the need for management of risk. No structured approach to dealing with uncertainty. Repetitive & reactive management processes Little or no attempt to learn from past or to prepare for the future	Experimenting with risk management through a small number of individuals. No generic structured approach in place. Aware of potential benefits of managing risk, but ineffective implementation, not gaining full benefits.	Management of risk built into routine business processes. Risk management implemented on most or all projects. Formalized generic risk processes. Benefits understood at all levels of the organization, although not always consistently achieved.	Risk-aware culture, with proactive approach to risk management in all aspects of the business. Active use of risk information to improve business processes and gain competitive advantage. Emphasis on opportunity management ("positive risk").
Culture	No risk awareness. Resistant/reluctant to change. Tendency to continue with existing processes.	Risk process may be viewed as additional overhead with variable benefits. Risk management only used on selected projects.	Accepted policy for risk management. Benefits recognized & expected. Prepared to commit resources in order to reap gains.	Top-down commitment to risk management, with leadership by example. Proactive risk management encouraged & rewarded.
Process	No formal processes.	No generic formal processes, although some specific formal methods may be in use. Process effectiveness depends heavily on the skills of the in-house risk team and availability of external support.	Generic processes applied to most projects. Formal processes incorporated into quality system. Active allocation & management of risk budgets at all levels. Limited need for external support.	Risk-based business processes. "Total Risk Management" permeating entire business. Regular refreshing & updating of processes. Routing risk metrics with constant feedback for improvement.
Experience/People	No understanding of risk principles or language.	Limited to individuals who may have had little or no formal training.	In-house core of expertise, formally trained in basic skills. Development of specific processes and tools.	All staff risk aware & using basic skills. Learning from experience as part of the process. Regular external training to enhance skills.

Application/ Technology	No structured application. No dedicated resources. No risk tools.	Inconsistent application. Variable availability of staff. Ad hoc collection of tools and methods.	Routine & consistent application to all projects. Committed resources. Integrated set of tools and methods.	Second-nature, applied to all activities. Risk-based reporting & decision making. State-of-the-art tools and methods.