ENTERPRISE RISK MANAGEMENT POLICY
AND
GOVERNANCE FRAMEWORK

Table of Contents

1 Introduction 4
1.01 Purpose 4
1.02 Scope 4
1.03 Abbreviations and Definitions 4
2 Policy Objectives 5
2.01 Risk Management Goals and Objectives 5
2.02 ERM Principles 5
3 ERM Governance Structure 6
3.01 Overview of Governance Structure 6
3.02 Three Lines of Defense 6
4 Role and Responsibilities 8
4.01 Board of Directors 8
4.02 Audit and Risk Management Committee 8
4.03 Management Team 9
4.04 Process/Risk Owner 10
4.05 Team Members 11
4.06 Quality Assurance 11
4.07 Risk Officer 12
4.08 Internal Audit 13
5 Enterprise Risk Assessment 14
5.1 ERA Procedures 14
5.1.1 Inputs 14
5.1.2 Business Objectives 14
5.1.3 Risk Groups 14
5.1.4 Risk Universe and Definitions 15
5.1.5 Risk Rating Criteria 16
5.1.6 Steps to perform an ERA 16
5.2 Emerging Risk Management 16
5.2.1 Emerging Risk Identification 16
5.2.2 Analysis and Scenario Development 18

5.2.3 Formulate an emerging risk strategy 19
5.2.4 Implement the Strategy 19
5.2.5 Monitor and report on the Strategy 20
6 Risk Appetite 21
6.01 Overview 21
7 Risk Reporting 22
7.01 Overview 22
7.02 Risk Master Sheet 23
7.03 Risk Heat Map 24
7.04 Risk Register 24
7.05 Key Risk Indicators 25
7.06 Audit Issue Tracker 25
7.07 Internal Control Acceptance Form 26
7.08 Strategic Objectives Risk Assessment 26
7.09 Project Risk Assessment Tool 26
8 Risk Training 27
9 ERM Policy Review 27
Appendix A - Definitions 28
Appendix B – Risk Universe 30
Appendix C – Risk Definitions 31
Appendix D – Risk Rating Criteria 44
Appendix E – Steps to performing an ERA 47

1 Introduction

1.01 *Purpose*

Enterprise Risk Management (ERM) is defined as an organization's competency to manage uncertainty, and more effectively minimize threats and maximize opportunity. ERM is characterized by systematic management practices to assess, monitor and respond to risk (financial, operational, compliance and strategic) using an appropriate risk management framework.

This policy communicates the Lasco Manufacturing Limited's (LML or "the Company") approach to Enterprise Risk Management and clearly distinguishes between those responsible for

- Establishing risk policy and methodologies
- Managing risks including implementation of strategies to mitigate; and
- Providing assurance that risks are adequately identified, managed and monitored.

1.02 *Scope*

This policy applies to all areas of LML, including the Board of Directors, Management Team and all Employees.

1.03 *Abbreviations and Definitions*

A&RMC	Audit and Risk Management Committee
BOD	Board of Directors
ERM	Enterprise Risk Management
FC	Financial Controller
IA	Internal Audit
IT	Information Technology
IS	Information Systems
LDL	Lasco Distributors Ltd
LML	Lasco Manufacturing Ltd
MD	Managing Director
RMC	Risk Management Committee

Please refer to Appendix A for a list of terms used in this policy and their respective definitions.

2 Policy Objectives

2.01 *Risk Management Goals and Objectives*

The key objectives of LML's Enterprise Risk Management programme are to ensure that:

- Key risks that may impede the achievement of the Company's strategic and business objectives are proactively identified, monitored and mitigated.
- Process to identify, assess, manage and report on risks is consistent.
- Risk management decision-making for the entire Company is consistent with the Company's risk appetite and strategies.
- Risk management is embedded into LML's culture and business processes.
- Direct accountability for risk management is established and communicated throughout the Company

2.02 *ERM Principles*

The following represent the key principles governing LML's ERM Policy:

- **Tone at the top:** The Board of Directors, Board Committees and Management Team are committed to the proactive management of risks according to the risk management framework.
- **Integrated approach:** Risk management is integrated into all business processes inclusive of strategic planning, operational planning, performance management and change management.
- **Training:** The Company promotes risk management training and risk awareness among its Board of Directors, Management, Team Members and all stakeholders.
- **Risk ownership:** Clear ownership of risk accountabilities, responsibilities, duties and actions are established and communicated.
- **Application:** A common approach to risk management is in place to promote consistency in the assessment, monitoring and reporting of risk.
- **Responsive to change:** LML will respond timely and appropriately to external and internal events and changes to ensure that emerging risks are accurately identified and previously identified risks are reassessed as needed.

3 ERM Governance Structure

3.01 *Overview of Governance Structure*

The Company has established a risk management governance framework which is consistent with best practice of sound risk management practice and includes the following:

- Clear structure of accountability, roles and responsibilities, and the segregation of duties through the application of the '*three lines of defense'* model.
- Closer alignment of risks and explicit consideration of risk into decision-making and performance management.
- Holistic risk management through harnessing synergies of the different functions involved in risk management.

3.02 *Three Lines of Defense*

In keeping with the *three lines of defense* model (see diagram on next page), LML distinguishes among three groups (or lines) responsible for effective risk management:

- **1st Line of Defense** – Departments are responsible and accountable for the ongoing management of risks including the identification, assessment and reporting of risk.
- **2nd Line of Defense** – Risk Management and compliance functions will oversee risk and challenge the completeness and accuracy of risk assessments, reporting and mitigation activities
- **3rd Line of Defense**– Independent Internal Audit function will review and provide objective assurance on the effectiveness of the Company's systems of internal controls.

The Board of Directors and Board Committees will be responsible for approving the risk management framework and providing oversight on a periodic basis (see also Section 4 Roles and Responsibilities).

ERM POLICY AND GOVERNANCE STRUCTURE

Management Team/ Board of Directors

Perform Oversight

Establish Risk Management Framework and provide Oversight

- Establishes risk appetite and strategy
- Approves the risk management framework, methodologies, policies, roles & responsibilities
- Sets "tone from the top"
- Leverages risk information into decision making process for risk identification and mitigation

Internal Audit

Test and Verify

Provide Assurance

3rd Line of defense – "Independent Assurance and Validation"

- Provides independent testing and verification of efficacy of corporate standard and business line risk management and compliance
- Validates the overall risk framework
- Provides assurance that the risk management process is functioning as designed and identifies improvement opportunities

Risk Officer

Design, Implement, Monitor and Report

2nd Line of defense – "Risk Control and Monitoring"

- Assist in the design and deployment of the overall risk management framework
- Monitors adherence to framework and strategy
- Escalates risk and control issues to Management and the Board
- Performs risk reporting
- Maintains risk management policies

Quality Assurance

Design, Implement, Monitor and Report

2nd Line of defense – "Risk Control and Monitoring"

- Monitor the manufacturing processes for compliance with standards at both national and international level
- Determining, negotiating and agreeing on in-house quality procedures, standards and specifications
- Setting customer service standards
- Specifying quality requirements of receipt and storage of raw materials

LML

Process/Risk Owner

Team Members

1st Line of defense – "Process/Risk Owner"

- Accountable for a risk area (process, IT application, asset, information, etc.)
- Identifies, assesses, manages and mitigates assigned risk
- Tracks, analyzes and reports on risk events on a periodic basis
- Updates risk registers and risk profiles

1st Line of defense – "Team Members"

- Understand all applicable policies and procedures
- Understand the key risks and controls related to their areas of responsibility
- Support Line Manager/Risk owner in ensuring that controls are designed and operating effectively

4 Role and Responsibilities

4.01 *Board of Directors*

The Board has overall responsibility for approving and overseeing the implementation of LML's strategic objectives, governance framework, corporate culture and values. The Board shall exercise their "duty of care" to LML under applicable laws and supervisory standards. On an ongoing basis, the Board's role is to:

- Set the "tone from the top" and promote a safe and sound risk culture.
- Establish business strategy (strategic plan) incorporating risk appetite and capital management activities.
- Approve the risk management framework, methodologies, policies, roles and responsibilities.
- Regularly receive and review key risk management information and provide timely feedback including challenging decisions made by management, where applicable.
- Provide an independent evaluation of the risk management governance and framework.

4.02 *Audit and Risk Management Committee*

The Audit and Risk Management Committee (A&RMC) shall be responsible for ensuring good fiscal discipline, open and accurate financial reporting and timely disclosure as part of our mandate to adhere to good corporate governance standards as well as the requirements of the Jamaica Stock Exchange on which LML is listed.

The A&RMC plays a key role in ensuring that the LML Risk Management Framework is implemented in accordance with the ERM Policy and its responsibilities shall include the following:

- Review and approve changes to LML's Risk Management Policy prior to submission to the BOD for ratification.
- Review and approve LML's risk appetite and limit framework prior to submission to the BOD for ratification.

- Review and monitor all financial, operational, compliance and strategic risks as identified and prioritized by Management, including emerging risks that may arise from time to time.
- Review and monitor risk tolerance levels and where necessary recommend action plans to remain within, or correct any deviations from, tolerance limits.
- Review recommendations from management with respect to the acceptance of any internal control deficiencies identified by either Internal or External Audit.

4.03 *Management Team*

The Management Team (also referred to as the Risk Management Committee or RMC) will provide ongoing oversight and support for the overall risk management framework. It is charged with the responsibility for reviewing and where necessary recommending changes to the Risk Management Framework to the A&RMC/BOD for approval. The Management Team (through the Risk Officer) will also escalate significant risk issues to the BOD as needed. Specific roles and responsibilities include, but are not limited to:

- Establishing a sound risk awareness culture throughout the Company.
- Establishing risk policies and providing ongoing guidance for refinement of the overall risk management framework.
- Formalizing risk appetite and tolerance (including review of draft appetite statements to be submitted and recommended for Board approval).
- Extending the risk appetite and tolerances to its strategic transactions/initiatives.
- Implementing procedures and processes, including those recommended by the Risk Officer, Quality Assurance Team or Internal Audit to identify the present and emerging risks, and to assess, control, monitor and report them.
- Assessing and validating the most significant financial, operational, compliance and strategic risks, including:
  - Participation in the enterprise risk assessment
  - Prioritization of risks and approval of the aggregated risk profile
  - Review and challenge actions on the risk profile and risk strategy

- Assigning risk owners to each risk
- Approving action plans and resource allocation
- Monitoring and control of these risks

- Periodic review and revision to the risk universe, risk profile, risk registers and risk response strategies.
- Oversight, review and deliberation of risk exposures vs. risk appetite and limits, and taking actions necessary to address deviations from tolerance.

4.04 *Process/Risk Owner*

The Process or Risk Owner plays a key role in LML's first line of defense and is responsible for identifying and assessing risks for their respective areas as well as implementing the appropriate actions or controls to mitigate the likelihood of occurrence and impact of the risk to LML.

Given that ERM is an integrated process, Risk Owners have the responsibility of understanding the key controls implemented to mitigate the risk even if they are not responsible for the operation of the control. Other responsibilities include:

- Identify, assess and manage risks leveraging the ERM risk universe, risk criteria and policies
- Provide input on emerging risk identification and assessment
- Assess and prioritize risks in the context of the risk appetite and risk tolerances
- Evaluate on a periodic basis (using the risk classification guide) changes to the risk profile driven by changes in business models, initiatives, strategies and external events
- Update risk registers after each risk review
- Propose strategies to mitigate risks and monitor remediation activity
- Define measures to tie risk management to business performance
- Provide quarterly reports to the Management Team on the Key Risk Indicators assigned including proposed action plans to address instances where actual exposure exceeds established tolerance or limits

4.05 *Team Members*

All employees, fixed term contractors and third-party contractors that play a key role in LML achieving its business objectives are classified as Team Members and form part of LML's first line of defense for risk management given their role in executing day to day controls that mitigate business risk. Specifically, each Team Member shall be responsible for the following:

- Exhibit a high level of integrity and ethics including adherence to LML's Code of Conduct
- Understand all company-wide policies and procedures as well as those applicable to their area of responsibility
- Understand the key risks that affect their area and the key controls to mitigate these risks.
- Support their Line Manager, Head of Department, Process/Risk Owner in ensuring controls are designed and operating effectively.
- Report to the Line Manager, Head of Department, Process/Risk Owner or Risk Officer of instances where key controls are no longer operating effectively or where new risks have emerged for which Management should be made aware and appropriate action taken.

4.06 *Quality Assurance*

As one of the critical elements of the 2nd line of defense for risk management, the Quality Assurance function plays a critical role in the design, implementation and monitoring of processes related to Good Manufacturing Practices (GMP), Hazard Analysis Critical Control Points (HACCP) and compliance with local laws and regulations governing the Manufacturing Industry. In addition, the following provides guidance with respect to other areas of risk management responsibility of the Quality Assurance function:

- Understand any changes to laws and regulations that affect LML's core manufacturing processes and provide support to the business in implementing such changes.

- Perform quality assurance checks/procedures to ensure compliance to GMP, HACCP and compliance with local laws and regulations governing manufacturing
- Provide on-going training and awareness to members of staff on GMP, HACCP and other related areas of compliance
- Act as liaison for any inspections/audits performed by regulatory agencies
- Monitor and report on the progress of remediating any deficiencies raised during a regulatory or QA audit/inspection

4.07 *Risk Officer*

The Risk Officer[1] forms the other part of LML's 2nd line of defense and has primary responsibility for overseeing the development and implementation of the risk management framework in collaboration with the LML Management Team. Specially, the Risk Officer will be responsible for the following:

- Assisting the Managing Director and Financial Controllers in establishing and implementing a risk management framework aligned to LML's strategic plan and risk appetite.
- Provides support to the LML Management Team and key stakeholders in ensuring the ERM framework is effectively embedded in the organization through the periodic review, identification, assessment, monitoring and reporting of risks.
- Ongoing monitoring and reporting of the risk-taking activities and risk exposures to the Management and the Audit and Risk Management Committee
- Performs a formal Enterprise Risk Assessment at least once every 3 years.
- Reviews current ERM framework and where applicable applies continuous improvement opportunities.
- Provides risk management training and awareness to the LML Management Team and all Team Members.

[1] Where LML does not have a specific Risk Officer role, the Managing Director has authority to nominate one or more persons to assume the duties of the Risk Officer.

4.08 *Internal Audit*

The Internal Audit reports directly to the Audit and Risk Management Committee and acts as the 3rd line of defense in the Governance Framework. The function shall provide independent assurance to the Board and Management Team on the quality and effectiveness of the internal controls, risk management and governance processes. Specific responsibilities of Internal Audit function include:

- Independently assessing the effectiveness and efficiency of internal controls, risk management and governance processes in accordance with international professional standards to provide assurance that it is functioning as designed.
- Identifying opportunities to improve the LML's internal controls, risk management and governance processes.
- Reviewing the risk registers prepared by the departments to determine whether risks are being appropriately addressed and reported in a timely manner.
- Validating the suitability and effectiveness of the controls put in place to mitigate risks and promote risk awareness.
- Developing the Internal Audit plan using the output of the Enterprise Risk Assessment in order to provide the Board/Audit Committee with independent assurance that the significant risks are being appropriately managed

5 Enterprise Risk Assessment

An enterprise risk assessment (ERA) is a defined process to assess, identify and prioritize risks and forms a critical component of the ERM Framework. The ERA should be performed at least once every two years utilizing the guidelines that have been documented in this policy.

5.1 ERA Procedures

5.1.1 Inputs

Several key inputs are to be considered when conducting the ERA for LML, such as the business objectives, risk groups, risk universe, risk definitions and risk criteria. These inputs need to be consistently defined and applied across the Company and serve as the "common language" for the risk assessment. They also need to be continuously re-evaluated and updated as appropriate

5.1.2 Business Objectives

Risk is the threat that an event, action, or non-action could affect the LML's ability to achieve its business objectives and execute its strategies successfully. Consequently, the risk assessment begins with an understanding of the Company's strategic objectives.

5.1.3 Risk Groups

Four primary risk groups have been identified, which may include one or more risk category as follows:

1) **Strategic** - risk related to the achievement of the LML's overall strategic objectives, whether it is the risk of not achieving/exceeding the strategy; or risks caused by adopting the strategy; or the risk of adopting the wrong business strategy.
2) **Operations** – risk of losses resulting from inadequate or failed internal processes, people and systems.

3) **Compliance** - risk of failing to operate within accepted corporate governance standards; manufacturing, legal, regulatory and compliance standards.

4) **Financial** – risk of failing to implement a robust and adequate financial strategy; or that cash flows and financial risks are not managed cost-effectively to (a) maximize cash availability, (b) reduce uncertainty of currency, interest rate, credit and other financial risks, or (c) move cash funds quickly and without loss of value to wherever they are needed most.

Risks are first assessed at an inherent risk level and then prioritized on a residual risk basis after considering the effectiveness of mitigating controls and management actions:

- **Inherent risk** – is the risk that is intrinsic to the business operations in the current environment but before considering risk management and control activities.
- **Residual risk** – is the risk remaining after considering existing risk management initiatives, processes, controls and performance measures used to manage the risk i.e., what is the reduced level of risk after inherent risk has been offset by all risk management activities and controls.

5.1.4 Risk Universe and Definitions

LML's risk universe defines all material risks which affect the entity. It is a common set of risk categories and definitions which has been approved for use within LML. This will promote use of a common risk language, improved understanding of risk and the ability to consolidate risk information.

The risk universe and associated risk categories should be continually updated during the coordination and implementation of ongoing risk assessment efforts, to reflect the dynamic risk environment of the Company. Subsequently, the risk universe categories and definitions are revalidated through the enterprise risk assessment and updates to the risk register.

Please refer to Appendix B for the LML Risk Universe and Appendix C for the associated risk definitions.

5.1.5 Risk Rating Criteria

All assessments of risk are based on how a potential event or circumstance would affect the ability of LML to achieve its business objectives. This uncertainty is expressed in terms:

- the likelihood of the risk occurring
- the impact of the risk should it occur
- the effectiveness of management actions and controls in place to mitigate the risk

Please refer to Appendix D for the risk rating criteria used for LML.

5.1.6 Steps to perform an ERA

Detailed procedures for performing an Enterprise Risk Assessment have been included in Appendix E of this ERM policy.

5.2 Emerging Risk Management

Emerging risk management is a forward-looking process that aims at identifying existing and probable events, trends and drivers that may change LML's risk profile. Given the limitations in data or experience relating to the risk, emerging risk identification requires strategic thinking and scenario planning

Emerging risk management consists of five primary activities:

1) Emerging risk identification
2) Analysis and scenario development
3) Formulate emerging risk strategy
4) Implement the strategy
5) Monitor and report on emerging risks

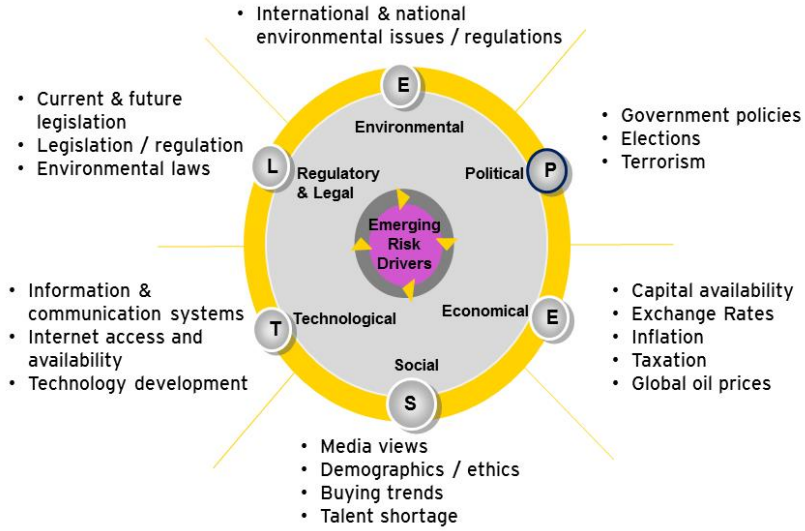
5.2.1 Emerging Risk Identification

Emerging risk identification is a continuous process of scanning the internal and external environment to identify potential threats, opportunities or drivers that could affect the Company. Methods used to identify early warning signs can be a combination of:

- Utilizing predefined lists of emerging risks and opportunities published by national/international entities and professional firms
- Scanning social media for key words and trends in public perception that can be further analyzed
- Assembling a panel of senior resources, with expertise in various fields, such as economists, compliance, legal, electronic channels, information security and credit risk who will provide regular input about forthcoming changes

When scoping the external environment, utilize a PESTLE analysis to identify emerging risks using the following drivers:

1) Political
2) Economical
3) Social
4) Technological
5) Regulatory/Legal
6) Social



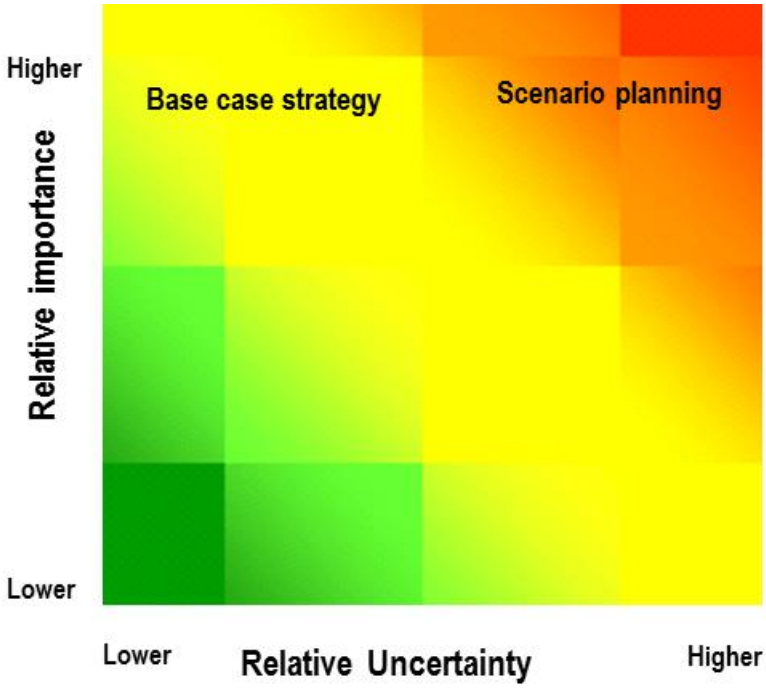
Filtering the list of early warning signs may be necessary to make efficient use of time. Factors to be considered when filtering include:

- Possible impact to LML's core values and business strategy
- Estimated likelihood of a threat to materialize
- Lead time before the threat/opportunity becomes reality
- Public awareness levels

On completion of this step, a plausible list of emerging risks should be available and put forward for further analysis.

5.2.2 Analysis and Scenario Development

The filtered list of early warning signs will be further analyzed by considering the relative importance and uncertainty of the emerging risk. This analysis can be plotted on a heat map to illustrate the priority of each risk and the action to be taken depending on the results.



Emerging risks that are assessed as having higher importance and lower uncertainty should be addressed by developing a base case risk mitigation strategy. Risks that are assessed as relatively important but highly uncertain should be subject to scenario analysis and planning. The concept of scenario analysis involves developing possible stories about how a particular event could unfold and identifying the drivers that lead to an event becoming a risk to be managed or an opportunity to be pursued.

Principles for scenario modeling:

- "Worst-case" should be considered to capture the full range of possible outcomes
- Biases should not be introduced into constructing the scenario as this can limit consideration of other plausible outcomes
- Scenario descriptions should be comprehensive to enable informed decision making. Care should be taken to carefully define the assumptions, critical events and contributing factors to the emerging risk in order to evaluate possible impact
- Scenarios should be re-defined as new information arises

5.2.3 Formulate an emerging risk strategy

A risk management strategy must be defined for each identified scenario and may include:

- Implementation of controls to mitigate against known drivers that contribute to the risk emerging
- Avoid the risk until increased knowledge is available
- Adapt risk appetite to the new risk, i.e., retain the risk and set aside funds to compensate for a potential future loss
- Take no action if the emerging risk, at the point in time, is not assumed to have any impact on the Company

Risk management strategies are influenced by the certainty surrounding the emerging risk. For example, if there is little knowledge of the emerging risk but it is expected to have negative consequences, a risk avoidance strategy is recommended until more information is available. If an emerging risk is well known, LML can either adjust their risk appetite or implement controls to mitigate against the drivers to the risk.

5.2.4 Implement the Strategy

When implementing the selected strategy, communication, clear delineation of roles and responsibilities and appropriate metrics or checkpoints, should be established.

- Communication of the description of the emerging risks, the known controllable factors, justification for the selected strategy, changes to the risk appetite (if applicable) and its effect on decision making are necessary for effective implementation. In addition, bottom up feedback may be required to reinforce support for the strategy and to solicit input from employees as to any unaddressed weaknesses. External communication may be required if other companies will be affected in a similar manner and can benefit from the exchange of information
- Roles and responsibilities should be clearly articulated. Risk ownership may need to be reviewed and reassigned, risk culture may shift and continuous monitoring roles may need to be established
- Metrics should be defined to monitor the emerging risks and to highlight checkpoints at which the emerging risk strategy should be revisited. In addition, there should be continuous monitoring to changes in the environment which will also drive a change in strategy

5.2.5 Monitor and report on the Strategy

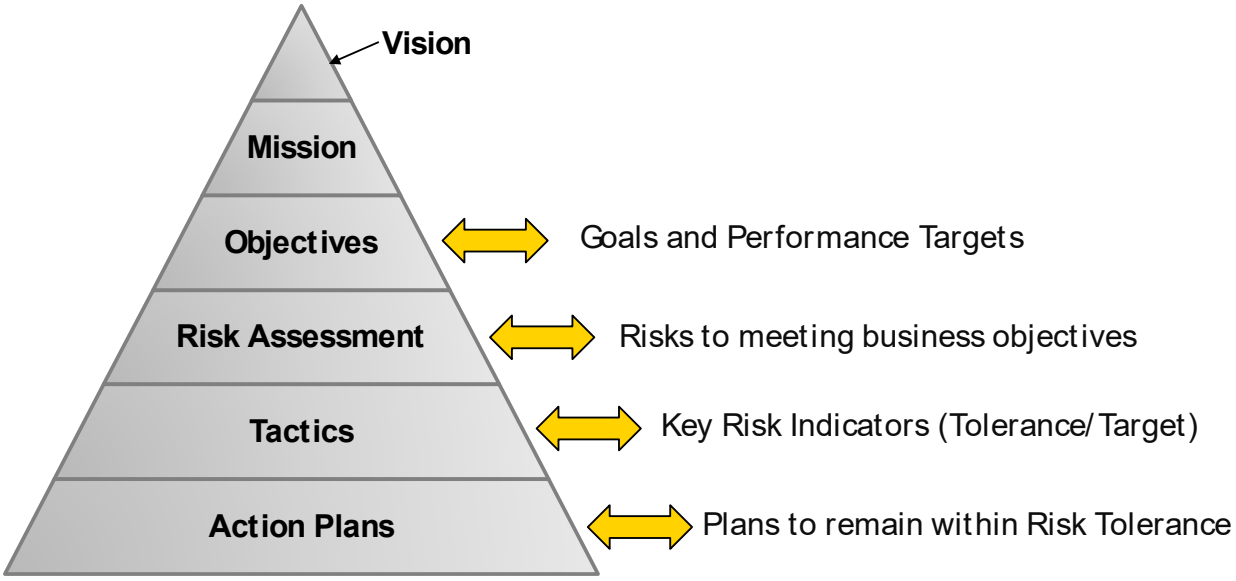
Emerging risk identification and treatment is an iterative process. Emerging risks, even those previously identified and addressed, should be continuously monitored. Also, monitoring the effectiveness of strategies used in avoiding losses can help inform future decision making.

On a quarterly basis, the Risk Officer is charged with the responsibility for reporting on emerging risks to Management and the Audit Committee. Reporting should include the emerging risk, its definition, drivers and risk management strategy.

6 Risk Appetite

6.01 Overview

A successful Enterprise Risk Management (ERM) Framework is one that is clearly integrated with the organization's strategy and provides a basis by which Management can focus on managing the risks that matter most in pursuit of its objectives with better predictability and consistency in performance.



Risk appetite is defined as the amount and type of risk that an organization is prepared to pursue, retain and take in pursuit of its strategic objectives. Articulating, communicating and monitoring the Company's risk appetite are integral components of the Risk Management Framework and is the basis for decision-making by the Management Team and the Board.

The LML Risk Appetite Statements and associated Key Risk Indicators are required to be reviewed on at least an annual basis and updated to reflect any changes in LML's overall risk appetite. Please refer to the LML Risk Appetite and Limit Framework for further details or contact the LML Risk Officer for further information.

7 Risk Reporting

7.01 Overview

Risk reporting is a critical element of the enterprise risk management framework as it provides the Management and Audit Committee with the information needed to make sound decisions that align with the Company's risk appetite and business objectives. The following are key principles to guide effective risk reporting.

- **Comprehensive**: Reports should cover all material risks affecting LML.
- **Timely**: Reports should be produced in a timely manner and circulated with a frequency appropriate to the risks. Certain risks should be monitored more frequently than others and specific events should trigger additional reporting outside of normal schedules.
- **Forward-looking**: Effective reporting should contain forward-looking elements and not just point-in-time.
- **Integrated**: Risks should be assessed across business and risk types on an integrated basis to identify Company-wide sensitivities and concentrations. Siloed reporting often leads to a misunderstanding of risk relationships.
- **Appropriate and relevant**: The reports should be geared to a level appropriate to the audience.
- **Qualitative and quantitative**: Avoid undue reliance on statistical estimates that can create a false sense of quantitative precision. Both quantitative and qualitative approaches should be used and informed judgment applied as to how they support planning and decision-making.

A number of templates have been created to provide end users with the tools and techniques to manage risks. A synopsis of each template and the reporting frequency is provided in the proceeding sections.

7.02 Risk Master Sheet

The Risk Master Sheet is a listing of all the risks in the LML Risk Universe and the latest risk rating scores for likelihood, impact and management control. In addition, this template provides the user with the following information:

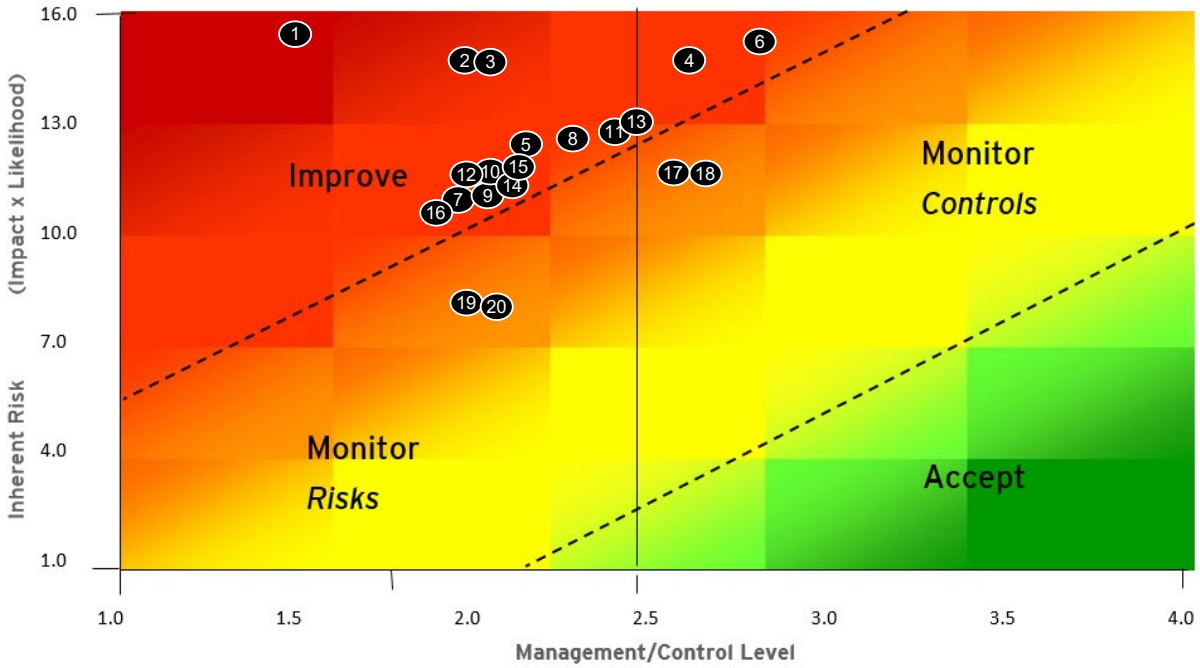
- Risk owner
- Risk register that the risk can be found
- Risk ranking (based on residual risk score)
- Risk response (i.e. Improve, Monitor Risk, Monitor Control, Accept)
- Frequency of review

The Risk Master is only to be maintained by the Risk Officer to protect the integrity of the risk scores. Risk Owners (or their delegate) are, however, required to review the risk register on at least a quarterly basis to identify their risk assignments and the frequency of the risk review. The following table provides a guide with respect to the frequency of the risk review:

Risk Classification	Description	Frequency of Review	Management/Board Review
Tier One Risks	Top 10 Risks	Quarterly	Risk Profiles presented to the Management Team and Audit Committee on a quarterly basis.
Tier Two Risks	Risks 11-20	Quarterly	Only if new risk rating scores places risk in the top 10 or at the discretion of the Management Team
Tier Three Risks	All risks outside of Top 20 with a "Monitor" type	Semi Annual	Only if new risk rating scores places risk in the top 10 or at the discretion of the Management Team
Tier Four Risks	All risks with an "Accept" risk response	Annual	Only if new risk rating scores places risk in the top 10 or at the discretion of the Management Team

7.03 Risk Heat Map

The Risk Heat Map provides a graphical representation of LML's top 20 risk and the extent to which key risks are being managed in the business. This Heat Map is to be maintained by the Risk Officer and presented to the Management Team and Audit Committee on at least a quarterly basis.



7.04 Risk Register

A risk register provides the risk owner with the ability to capture the key elements of a risk, i.e. the risk characteristics or drivers, the key controls or management actions to mitigate the risk and the improvement opportunities to be undertaken. The Risk Register has built in Risk Profiles that facilitates ease of reporting to the Management Team or Audit Committee.

LML Risk Registers are available for review and update by the Risk Owner and can be found on the Risk Management SharePoint. For further information please contact the LML Risk Officer.

7.05 Key Risk Indicators

Key risk indicators are business metrics used to monitor risk exposure within the Company. Key Risk Indicators have been created based on the Company's Risk Appetite and limit framework. A complete list of all Key Risk Indicators can be found in the LML Risk Appetite Framework document on the Risk Management SharePoint.

It is the responsibility of the Risk Owner to track the actual results of Key Risk Indicator for which they are responsible for. The Risk Officer is responsible for collating and reporting on all Key Risk Indicators to the Audit Committee on a quarterly basis.

7.06 Audit Issue Tracker

The Audit Issue Tracker provides Management with an overview on how high and medium risk issues raised by Internal Audit or External parties are being managed. External parties may include LML's External Auditors, Bureau of Standards, National Environmental Planning Agency, Water Resources Authority, Ministry of Industry and Commerce, etc.

The Risk Officer will be responsible for tracking the progress to completion for all Internal Audit matters and updating the Audit Issue Tracker accordingly. The Financial Controller (or delegate) will assume responsibility for tracking risk issues raised by the LML External Auditors while the Quality Assurance Manager (or delegate) will be responsible for tracking all other high/medium risk issues raised via regulatory audits or inspections. The Audit Issue Tracker will be presented to the Audit Committee quarterly by the Risk Officer

Where an extension to the expected completion date is required, it will be the responsibility of the person assigned to the action to provide the rationale for the change in the completion date and to seek approval using the following guidance:

- External audit or finance related issues – approval from the Financial Controller is required
- Quality Assurance or Regulatory audit issues – approval from Quality Assurance Manager is required
- Production related issues – approval from the General Manager is required
- All other audit issues – approval from the Managing Director is required

7.07 Internal Control Acceptance Form

Where a control weakness (and associated recommendations) have been raised by the Internal Audit Team for which Management is either (a) unable to implement due to cost, timing or system limitations or (b) of the opinion that current mitigation efforts are adequate to address the risk, then it is incumbent on the Management Team member responsible for the issue to complete the Internal Control Acceptance Form and provide the rationale for the issue to be accepted.

The Internal Control Acceptance Form will be presented to the Audit Committee (by the Risk Officer) for review and approval at the next sitting of the Audit Committee.

7.08 Strategic Objectives Risk Assessment

This template can be used to perform an initial risk assessment for key projects or initiatives that support the achievement of LML's Strategic Objectives. It allows Management to get an indication of which projects or initiatives have a higher degree of risk and hence would need to either be improved in relation to its risk management activities, monitored consistently to prevent project deviations or accepted on the basis that current measures should be adequate to ensure a successful project delivery without the need for additional intervention.

Assessment templates are available on the Risk Management SharePoint.

7.09 Project Risk Assessment Tool

This template can be used to perform a risk assessment for key projects or initiatives that are being undertaken and provides management with an understanding of how project risks are being managed. Assessment templates are available on the Risk Management SharePoint.

8 Risk Training

LML will foster a high-performance risk culture through continuous risk management training for the Board, the Management Team and select Team Members. New Team Members will be introduced to the Risk Management Framework during their orientation process. Risk management training will range from general risk awareness sessions to specific training on risk identification, monitoring and reporting.

Risk management training will be the joint responsibility of the Risk Officer and the Human Resources Manager.

9 ERM Policy Review

The Risk Officer is responsible for reviewing the ERM Policy and Governance Framework on an annual basis. All recommendations for amendments are to be submitted to the Management Team for review prior to submission to the Audit Committee for approval and subsequently to the Board of Directors for ratification.

Changes made to the ERM policy and any associated risk management policies (e.g. risk appetite and limit framework) will be communicated to all stakeholders by the Risk Officer.

Appendix A - Definitions

In adopting a standard approach to risk management, the definitions for the following terms have been provided in the table below to drive consistency in communication and build stakeholder awareness:

Term	Definition
Control	Policy, procedure or action taken to mitigate the likelihood of occurrence or the impact of a risk
Enterprise Risk Management (ERM)	Organization's competency to manage uncertainty and more effectively, minimize threats and maximize opportunity
Inherent Risk	The risk level or exposure without considering the actions that management has taken or might take (e.g., implementing controls)
Key Risk Indicators (KRIs)	A subset of risk indicators that are highly relevant and possess a high probability of predicting or indicating important risk
Likelihood	The probability of something happening
Level of risk	The acceptable level of risk that management is willing to tolerate for any particular risk as the enterprise pursues its objectives. This can be measured quantitatively and qualitatively.
Monitoring	To determine the current status and to assess whether or not required or expected performance levels are actually being achieved.
Residual risk	The remaining risk after management has implemented a risk response
Risk Review	The process of identifying potential problems before they occur so that risk-handling activities may be planned and invoked as needed across organization or project to mitigate adverse impacts on achieving objectives.
Risk	The combination of the probability of an event and its consequence
Risk analysis	The initial steps of risk management which involves analyzing the value of assets to the business, identifying threats to those assets and evaluating how vulnerable each asset is to those threats

Term	Definition
Risk appetite	The aggregate level and types of risk an organization is willing to assume, decided in advance and within its risk capacity, to achieve its strategic objectives and business plan.
Risk assessment	A process used to identify and evaluate risk and its potential effects
Risk culture	An organization's norms, attitudes and behaviors related to risk awareness, risk-taking and risk management, and controls that shape decisions on risks. Risk culture influences the decisions of management and employees during the day-to-day activities and has an impact on the risks they assume.
Risk capacity	The maximum amount of risk an organization can assume given its capital base, risk management and control capabilities as well as its regulatory constraints.
Risk evaluation	The process of comparing the estimated risk against given risk criteria to determine the significance of the risk.
Risk identification	the process of determining risks that could potentially prevent the program, enterprise, or investment from achieving its objectives
Risk Impact	The process of assessing the probabilities and consequences of risk events if they are realized.
Risk owner	The person in whom the organization has invested the authority and accountability for making risk-based decisions and who owns the loss associated with a realized risk scenario
Risk profile	Point-in-time assessment of an organization's gross risk exposures aggregated within and across each relevant risk category based on current or forward-looking assumptions.
Risk rating	The acceptance criteria for risk value qualitatively illustrated using three distinct levels for risk: Low, Medium, and High.
Risk Register	A repository of the key attributes of potential and known risk issues
Risk tolerance	The acceptable level of variation that management is willing to allow for any particular risk as the enterprise pursues its objectives

Appendix B – Risk Universe

Strategic

Governance:
- Board Performance/Tone at the Top
- Culture
- Control Environment
- Policies and Procedures
- Corporate social responsibility
- Brand Image

Communication:
- Media relations
- Employee Communication
- Investor relations
- Crisis Communication

Major Project:
- Project Planning and Execution
- Technology implementation
- Change Management
- Identify and Execute Opportunities

Market Dynamics:
- Macro-Economic factors
- Negative Taxation or Legislation
- Socio-political
- Lifestyle Trends/ competition

Planning and Forecasting:
- Strategic Planning
- Forecasting and Budgeting
- Outsourcing arrangements
- Tax strategy and planning

Operations

General Operating Controls:
- Records Retention
- Health, Safety and Security
- Asset Management
- Natural and Man-Made Disasters
- Insurance

HR:
- Recruitment and Retention
- Development and Performance
- Succession Planning
- Internal fraud
- Disciplinary hearings, appeals and grievances

IT:
- IT Resource and Support Management
- Application development and Maintenance
- Data governance /data integrity
- IT Infrastructure/ architecture
- IT reliability and recovery
- IT and Data Security

Sales and Marketing:
- Marketing and Advertising
- Sales Execution
- Trade Promotions
- Innovation
- New Product Development and Planning
- Pricing

Operations

Supply Chain (Plan, Procure, Manage):
- Master Planning and sales forecasting
- Procurement
- Warehouse Management
- Customs Clearance (AEO)

Supply Chain (Produce and Deliver):
- Manufacturing Efficiency
- Quality Assurance
- Environment
- Delivery /Dispatch
- Sales Returns

Compliance

Compliance:
- Regulatory Compliance
- Tax compliance
- Contracts
- Consumer protection (Mis- selling)
- Litigation
- Intellectual property

Financial

Financial:
- General Accounting
- Financial reporting and disclosure
- Equity
- Liquidity and Credit Management

Appendix C – Risk Definitions

Strategic Risks

Risk category	Key business Risk name	Description
GOVERNANCE	**Board Performance/Tone at the Top**	Failure of the Board of Directors to discharge their obligations and duties to the Company in good faith and establish, monitor and reinforce an environment that encourages integrity, ethical values, and competence of the Company's people through management's operating style, assignment of authority and responsibility.
	Culture	Failure to create and embed a set of values and accepted standards of employee behaviour that promote integrity and guide the desired level of performance/conduct may result in an increase in fraudulent transactions, corruption, operational inefficiencies and low employee morale.
	Control environment	Inability to establish and maintain an effective internal control environment which promotes proper financial reporting, operational efficiencies and achievement of the Company's strategic objectives may result in significant or material weaknesses, financial losses, regulatory breaches and sub-par operational performance.
	Policies and Procedures	Failure to establish, communicate and embed adequate policies and procedures in providing guidance to end users in the performance of core business processes may result in operational inefficiencies and financial losses due to poor execution and increased need for re-work.
	Corporate social responsibility	Inability to adequately promote or manage "socially responsible" activities may result in an unfavourable corporate perception with stakeholders, customers, suppliers, business partners, employees and the regulatory community.
	Brand Image	The risk that the Company does not recognize or appropriately manage reputation threats as perceived by investors, suppliers, customers, employees, and other key stakeholders.

Risk category	Key business Risk name	Description
COMMUNICATION AND INVESTOR RELATIONS	**Media relations**	Inability to anticipate and manage shifts in the information that stakeholders want and the way in which they want it communicated to them. Failure to provide effective and transparent communications with the public in order to create goodwill may result in negative publicity or inaccurate information being shared in the public domain.
	Employee Communication	Failure to understand and respond to the communication needs of different employees which results in a disconnected company with low levels of employee morale.
	Investor relations	Inability to provide relevant and accurate information in a timely manner to investors can result in loss of confidence.
	Crisis Communication	Inability to communicate the right message in an effective manner to recover and maintain business operations in the event of a crisis or disruption due to physical or natural circumstances.

Risk category	Key business Risk name	Description
MAJOR PROJECTS AND INITIATIVES	**Project Planning and Execution**	Failure to plan, execute and perform appropriate post implementation assessments and monitoring for major projects in a systematic manner which may result in financial losses, delays in project completion and inability to realize project benefits.
	Technology implementation	The risk that a major technology implementation fails to meet LML's strategic objectives. This also includes the risk that the Company does not use appropriate technology to achieve competitive advantage resulting in loss of market share, financial losses and operational inefficiencies.
	Change Management	The risk that the Company does not have effective and efficient processes for executing business and people change resulting in the inability to obtain acceptance and possible project failure.
	Identify and Execute Opportunities	Inability to identify, initiate and execute merger and acquisition opportunities in the market that are aligned to the Company's strategic objectives.

Risk category	Key business Risk name	Description
MARKET DYNAMICS	**Macro-Economic factors**	Inability to react to changes in macro-economic conditions such as increases in the inflation rate, volatility in foreign exchange and interest rates, changes in the global market, economic recessions etc., which may limit revenue generation (increase production and operating costs) and profitability (decreased returns on investment).
	Negative Taxation or Legislation	Imposition of negative tax or legislative measures on products which result in higher overall cost of sales, increase in selling price, lower demand or the inability to supply specific segments in the market.
	Socio-political	Exposure to social and political factors within a market environment that affect the ability to market, sell and service products and services.
	Lifestyle Trends/ competition	Failure to recognize new or evolving customer expectations driven by factors such as economic trends, technological advancements, demographic patterns, cultural concerns, competition, etc. which can result in dissatisfied consumers and potential loss of customers and consumers to competitors.

Risk category	Key business Risk name	Description
PLANNING AND FORECASTING	**Strategic Planning**	The risk that strategic planning and growth agendas are not properly developed, communicated or managed to achieve future performance expectations.
	Forecasting and Budgeting	Inability to effectively budget and forecast financial information for new and existing initiatives that support the overall strategic goals and objectives for growth, expansion, acquisition and overall profitability.
	Outsourcing arrangements	Inability to optimize business effectiveness and profitability through selecting appropriate outsourcing arrangements may result in financial losses and operational inefficiencies. Lack of management oversight of contracted third party service providers can result in financial losses, substandard service and operational inefficiencies.
	Tax strategy and planning	Inability to properly evaluate and execute tax planning strategies in order to optimize tax obligations consistent with business risk appetite.

Operational Risks

Risk category	Key business Risk name	Description
GENERAL OPERATING CONTROLS	**Records Retention**	The business may incur reputational damage and significant costs because it fails to keep, wrongly destroys or does not organise information so that it can be found in a timely manner.
	Health, Safety and Security	Employees or visitors are exposed to safety or security threats that result in actual injury/harm or create an atmosphere of fear resulting in employees not able to do their job.
	Asset Management	Failure to provide physical protection and stewardship over long-lived assets (such as buildings, furniture, fixtures, machinery, equipment and other assets) designed to optimize longevity and utilization.
	Natural and Man-Made Disasters	The risk that a natural (uncontrollable) and man-made event occurs, such as hurricane, earthquake, sabotage, fire etc., which impairs the Company's capability to sustain critical operations, provide products to the market and causes the Company to incur additional operating costs.
	Insurance	Inadequate insurance coverage fails to protect the company from significant financial losses arising from a disaster or other unexpected incidents and claims.

Risk category	Key business Risk name	Description
HUMAN RESOURCES/ PEOPLE	**Recruitment and Retention**	Failure to attract and/or retain employees with the requisite knowledge and experience may lead to operational inefficiencies and increased operating costs. Risk also includes the inability to compensate and provide benefits to employees that align with employee expectations and the competitive environment which may lead to employee dissatisfaction, high employee turnover and the inability to attract new talent.
	Development and Performance	Inability to develop and enhance employee skills and provide performance management to achieve organizational strategies, goals and objectives. This also includes the risk that clear accountability and responsibility has not been established and appropriately enforced due to a lack of adequate monitoring or appropriate consequences.
	Succession Planning	Failure to create and implement a succession plan for key organizational roles and talent resulting in loss of institutional knowledge, declining employee morale, inability to retain key talent and operational inefficiencies.
	Internal fraud	Losses due to acts intended to defraud, misappropriate property or circumvent regulations, the law or company policy which involves at least one internal party.
	Disciplinary hearings, appeals and grievances	The risk that employee/stakeholder appeals or grievances are not addressed in accordance with applicable requirements which may lead to reputational damage.

Risk category	Key business Risk name	Description
INFORMATION TECHNOLOGY	**IT Resource and Support Management**	The risk that the Company fails to adequately and effectively develop the requisite resources to enable business objectives and facilitate the efficient operation of the information technology function including effective support of end user needs.
	Application development and Maintenance	The risk that the Company fails to develop or purchase software applications that meet the needs of the business, or that the development of those applications (design, build, test and deploy) are not performed in accordance with appropriate IT change management methodologies.
	Data governance /data integrity	The risk that data integrity (e.g., completeness, accuracy and accessibility) is compromised as it is captured, processed, stored, summarized or reported by various systems deployed by the Company.
	IT Infrastructure/ architecture	The risk that the entity does not have a scalable and flexible IT infrastructure to capture, retain and transfer data in a secure and reliable environment. This risk also includes inadequate IT infrastructure to support current and future achievement of strategic business objectives with no monitoring of performance and capacity issues.
	IT Reliability and Recovery	The risk that existing applications, systems or data processing capabilities will not be available to end-users when needed or inability to recover critical data, programs, applications, and data processing capabilities in a timely manner following a business disruption.
	IT and Data Security	Failure to protect data, applications, systems (including online systems) and IT assets from theft, corruption, unauthorized usage, viruses, intrusion or sabotage which may lead to acts of fraud, loss of client information, business shutdown, decreased public confidence and potential shut down of the Company's operations.

Risk category	Key business Risk name	Description
SALES, MARKETING AND INNOVATION	**Marketing and Advertising**	Inconsistent, inappropriate, ineffective, or untimely marketing to customers or potential customers and the market which negatively impacts market share, revenue, and reputation.
	Sales Execution	Inability to create an effective sales and marketing plan to introduce new products, enter new markets or sell products to achieve the Company's strategic and financial goals.
	Trade Promotions	Inability to adequately plan, budget, monitor and evaluate trade promotional activities which result in ineffective use of the Company's resources and intended benefits not being realized.
	Innovation	Failure to innovate or generate new ideas (products) in a timely manner to capture market share and take advantage of competitive opportunities in the market place.
	New Product Development and Planning	Risk of possible errors, flawed assumptions or insufficient market research and analysis in proposing and pricing of new products as well as lack of appropriate approvals from internal and external stakeholders resulting in ineffective decision making, inability to meet objectives, delays in market launch and regulatory breaches.
	Pricing	Inability to price products correctly or competitively to achieve target margins.

Risk category	Key business Risk name	Description
SUPPLY CHAIN – PLAN, PROCURE, MANAGE	**Master Planning and sales forecasting**	Failure to properly forecast sales and inventory and prepare/execute a production plan than supports sales demand resulting in under or over production, inability to meet sales targets and financial losses due to working capital tied up in unsold inventory.
	Procurement	Failure to support LML's operational and financial objectives by defining and executing a world class procurement strategy and business plan which accounts for import and customs regulations, supplier selection; cost; inventory quality and contract supervision may result in financial losses, ineffective operations and reputational damage due to out of stock or poor product quality
	Warehouse Management	Failure to provide protection and stewardship over inventories (including raw materials and packaging materials) which may result in theft, obsolescence, contamination and breaches of regulatory requirements.
	Customs Clearance (AEO)	Failure to comply with the regulations as specified by the Jamaica Customs Agency resulting in LML losing its Approved Economic Operator status and further delays to the customs clearance process

Risk category	Key business Risk name	Description
SUPPLY CHAIN – PRODUCE AND DELIVER)	**Manufacturing Efficiency**	Inability to effectively implement manufacturing processes and practices to ensure that production inputs (raw materials, packaging materials and labour) are used in an optimal manner and production machinery is adequately maintained (with sufficient engineering spare parts available) to minimize breakdowns and other disruptions.
	Quality Assurance	Inadequate quality control measures, including failure to adhere to Good Manufacturing Practices, HACCP, ISO or BSJ standards, may result in the release of inferior products to the market and an increase in sales returns and product complaints.
	Environment	Failure to adequately assess and implement measures to minimize the impact to the environment as a result of manufacturing activities, including but not limited to carbon emissions, waste to landfill, water usage, effluent management, recycle non-bio degradable materials.
	Delivery /Dispatch	Shipments/deliveries are not approved or accounted for in a complete and accurate manner resulting in financial loss and possible fraud.
	Sales Returns	Failure to implement measures to minimize and/or manage sales returns as a result of product expiry, damage or other product quality issues.

Compliance Risks

Risk category	Key business Risk name	Description
COMPLIANCE	**Regulatory Compliance**	Failure to put measures in place to adhere to prescribed standards of local regulatory bodies and Acts, including the Bureau of Standards, the Factories Act, Ministry of Health, NEPA, etc which may result in fines, loss of certification and reputational damage.
	Tax compliance	Inability to identify and prevent risks posed by and/or non-compliance, with local jurisdictional and government rules and regulations for tax compliance that may result in legal fines, penalties, and lawsuits.
	Contracts	Formation and acceptance of contracts that are unfavourable to the company; and the failure to comply with and monitor contract terms to protect the company from financial losses.
	Consumer protection (Mis- selling)	The risk that consumers are treated unfairly or mis-representations made which may lead to reputational consequences and loss of market share.
	Litigation	Inability to comply with a responsibility, duty or obligation that may result in lawful consideration to provide satisfaction, compensation or other form of restitution. This includes the risk of various litigation actions, which, if resolved unfavourably, could result in substantial penalties and/or monetary damages and adversely affect the entity's financial position and reputation.
	Intellectual Property	Inability to define required parameters around the creation, capture, enhancement, leverage and protection of the collective knowledge, expertise and ideas of the Company may result in loss of competitive advantage.

Financial Risks

Risk category	Key business Risk name	Description
FINANCIAL	**General Accounting**	Failure to establish and implement appropriate procedures and policies to capture, record, process and monitor all relevant transactions (including related party transactions) in accordance with good accounting practices which can lead to financial misstatements and ineffective decision making.
	Financial reporting and disclosure	Financial reports issued to existing and prospective investors, lenders, and regulatory bodies are untimely, include material misstatements, omit material facts, or are not in compliance with applicable accounting and reporting requirements which can result in loss of stakeholder confidence, ineffective decision making and penalties and fines.
	Transfer Pricing	Good and services between related parties are transferred at prices that are inaccurately calculated This may result in ¢ increased tax thereby increasing cost of production and increasing profit.
	Equity	Failure to raise cash from investors and managing the return to investors through the number and type of share offerings as well as dividends.
	Liquidity and Credit Management	The risk that LML does not have sufficient resources (cash) available to meet its obligations as they fall due or can secure them only at excessive cost resulting in financial losses and loss of stakeholder confidence. Risk also includes inability to effective manage credit offered to its customers resulting in sub-optimal cash inflows.

Appendix D – Risk Rating Criteria

Criteria - Impact

RATING		FINANCIAL		OPERATIONS	COMPLIANCE	STRATEGIC	
		Losses	Disclosure	Operational Performance	Legal/Regulatory	Reputation	Strategy
4	Significant	> $35m Unplanned Loss/Write Off	Fiscal year restatement	➢ Significant unplanned Loss of production capability ➢ Product Recall ➢ Significant increase in complaints ➢ Serious injury resulting in loss of limb, eye or other appendage. ➢ Significant % of total production discarded due to quality issues ➢ 5 Key talent roles leave within a year ➢ Significant system downtime	➢ Loss of License to Operate ➢ Severe breach of local or international laws or regulations with significant penalties ➢ Severe breach of contract resulting in law suits and injunctions	➢ Complete loss of stakeholder confidence with Market share potentially irrecoverable (i.e. >24 months) ➢ Inability to establish new customers or manage existing relationships ➢ Adverse media coverage (social media and print) ➢ Governmental intervention	➢ Inability to execute strategy or strategic plan does not exist. ➢ Significant financial restructuring ➢ Potential acquisition or bankruptcy
3	Major	Between $21M and $35M unplanned loss/Write Off	Material deficiency	➢ Major unplanned Loss of production capability ➢ Significant product returns ➢ Major increase in customer complaints ➢ Serious injury with days lost greater than 30 days (no loss of limb or eye). ➢ Major % of total production discarded due to quality issues ➢ 4-5 Key talent leaves within a year ➢ Major system downtime	➢ Written reprimands threatening revocation of License to Operate ➢ Major breach of local or international laws or regulations with penalties imposed ➢ Major breach of contract resulting in law suits and injunctions	➢ Extensive decrease of stakeholder confidence – Market share recovery long term (i.e. 12-24 months) ➢ Increased difficulty in customer relationship management. ➢ Stakeholder comments in print and social media	➢ Severe problems with strategy execution ➢ Major financial restructuring

Criteria – Impact (Cont'd)

RATING		FINANCIAL		OPERATIONS	COMPLIANCE	STRATEGIC	
		Losses	Disclosure	Operational Performance	Legal/Regulatory	Reputation	Strategy
2	Moderate	Between $7m and $21m Unplanned Loss/Write Off	Significant deficiency not remediated within 30 days of due date	➢ Moderate loss of production capability ➢ Moderate increase in sales returns ➢ Moderate increase in customer complaints ➢ > 1 Loss Time Accidents in a 12-month period ➢ Moderate % of total production discarded due to quality issues ➢ 2-3 key talent roles leave within a year ➢ Moderate system downtime	➢ Moderate breach of local or international laws and/or regulations - written reprimand from regulators, no fine imposed, ➢ Written complaints	➢ Noticeable decrease of stakeholder confidence – Market share recovery mid-term (i.e. 6-12 months) ➢ Media coverage preventable through good public relations and customer relationship management	➢ Significant change to Strategic Plan
1	Minor	< $7m Unplanned Loss/Write Off	Significant deficiency or control weakness remediated within 30 days of due date	➢ Minor loss of production capability ➢ Minor increase in sales returns ➢ < 1 Loss Time Accidents in a 12-month period ➢ Minor % of total production discarded or disposed due to quality issues ➢ 1 or less key talent roles leaves within a year ➢ Minor system downtime	➢ Minor breach of local or international laws and/or regulations - verbal reprimand. ➢ Verbal complaints	➢ Minimal decrease of stakeholder confidence – Market share recovery mid-term (i.e. <6 months) ➢ Limited or no media coverage (social or Print media)	➢ Minor impact on strategy or minor changes to strategic plan

Criteria – Likelihood

RATING	RATING	OCCURRENCE	FREQUENCY	PROBABILITY
4	Almost Certain	Expected to occur in given circumstances	Would be expected to occur more than once per year	> 85% chance of occurrence
3	Likely	Likely to occur in given circumstances	Would be expected to occur once per year	Between 50% and 85% chance of occurrence
2	Possible	Event could occur at some time	Would be expected to occur within 1- 3 years	Between 15% and 50% chance of occurrence
1	Unlikely	Event could occur in rare circumstances	Would be expected to occur within 3- 5 years	Between <15% chance of occurrence

Criteria – Management Actions/Controls

RATING	CONTROL EFFECTIVENESS	MANAGEMENT'S ASSESSMENT
4	Effective (minor improvement opportunity)	Controls/risk management functions are properly designed and operating as intended, with minor opportunities for improvement identified. Low audit risk rating.
3	Moderately Effective (moderate improvement opportunity)	Controls/risk management functions are in place, with moderate improvements identified. Moderate audit risk rating
2	Ineffective (significant improvement opportunity)	Limited controls/risk management functions are in place. A high level of risk remains. High audit risk rating.
1	Highly Ineffective (critical improvement opportunity)	Controls/risk management functions are non-existent and don't operate as intended or major deficiencies exist. Extreme audit risk rating.

Appendix E – Steps to performing an ERA

Overview

The following summarizes the key activities when conducting an ERA (see section 5.0):

- **Identify risks and rating criteria –** this is the process of identifying, describing and categorizing risks that have the potential to impact the achievement of LML's strategic objectives. Key steps include:
    1) Review and revise (where necessary) LML's risk universe and rating criteria.
    2) Identify participants and distribute pre-read documents e.g. the **risk universe** and **risk rating criteria.**
    3) Perform the interviews (or administer surveys where necessary)
    4) Consider risks identified by internal and external assurance functions.

- **Analyze risks –** this is the process of determining the level of exposure. Key steps include:
    5) Populate risk register and generate risk profile.

- **Evaluate risks –** this is the process of prioritizing risks and agreeing action plans to be implemented. Key steps include:
    6) Update Risk Master
    7) Validate and prioritize risks
    8) Determine action items which will assist in mitigating risks

Step 1: Review Risk Universe and Risk Rating Criteria

The Management Team should align on the risk universe, the participants assigned to asses a specific risk and the risk rating criteria to be used to guide risk ratings. Risks are to be assessed in terms of likelihood and impact. Residual risk ratings are determined based on ratings assigned to the effectiveness of management controls.

Impact (Inherent risk)

The impact of the risk is rated from a scale of 1 to 4 (minor to significant). The severity of impact represents the level to which the risk, if it did occur, would impact the ability to deliver on business objectives, with impact measured on an annualized basis. Impact should include both quantitative and qualitative effects to measure the severity of the risk event with revenue and cost as the common financial denominators. These measures should be reviewed and amended as the business environment changes (at least on an annual basis).

Likelihood (Inherent risk)

The likelihood represents the probability of the occurrence of the potential event and is rated using a range from 'unlikely' to 'almost certain', with assigned numeric values from 1-4.

Contemplate the likelihood of a single event with a significant impact or multiple events of the same risk that would aggregate to or equate to a significant impact on an annualized basis. Attention should be paid to past occurrences in lines of business, the Company and those of similar industry peer organizations

Management and Control Activities (Residual Risk)

This is used to assess the effectiveness of existing controls to reduce the likelihood of the occurrence of a risk event. The rating scale is based on numeric values 1 to 4, which represents "highly ineffective' to 'effective' respectively.

Management and control activities include initiatives, policies and procedures, physical restrictions, guidelines, rules, insurance, etc.

Step 2: Distribute Pre-Read Materials

Participants should be submitted pertinent information to assist them in providing informed and value-added responses in identifying the key risks facing the Company. The documents distributed to the participants should include:

- Strategic plan or objectives for the current period
- Definitions of key risk terms
- The Risk Universe and definitions
- Risk Rating Criteria for Impact, Likelihood and Control Activities

Step 3: Perform interviews (or Surveys)

Capture participant feedback on the top risks facing LML as well as their respective risk ratings using the risk rating criteria. It is important to focus on the key characteristics of the risk (i.e. what would drive the realization of the risk from LML's perspective as well as the potential consequences of the risk), the key controls or actions to mitigate the risk as well as any improvement opportunities.

Step 4: Consider alternate risk identification methods

Apart from interview based discussions and surveys, consideration should be given to risks identified by internal and external assurance functions. Examples of information that can be incorporated into the identification process include:

- Results of financial and operational audits, compliance assessments etc.
- External reviews, including benchmarking, discussions with peers, external environmental monitoring and input from external parties.
- Where risks have previously been identified, this step will consist of confirming the completeness of the risks already identified, and considering changes in the current business, operating and control environment that may make previously identified controls redundant or may introduce new risks.

Step 5: Populate Risk Register/Profiles

In this step, the facilitator will update the risk registers with the risk rating scores as well as any information regarding the risk characteristics, mitigating activities and improvement opportunities. In deriving the scores to be used, the facilitator may opt to use the average scores of the participants given that the risk being assessed will be performed by a limited number of stakeholders.

The LML risk register template has built in formulas that calculate the inherent risk as well as the residual risk, the latter being the basis by which we rank risks (i.e. the higher the residual risk score, the greater the risk priority).

The formula that is used to derive the **inherent risk ratings** is as follows:

Inherent Risk = ((Impact x Likelihood)

The formula that is used to derive the **residual risk ratings** is as follows:

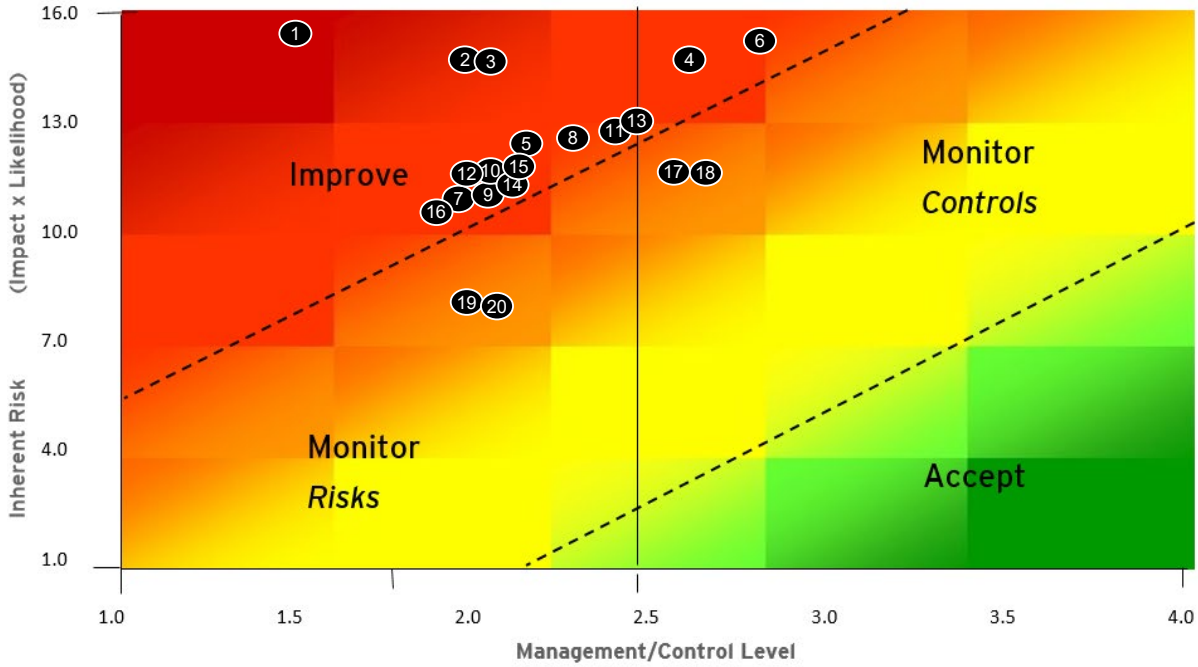
(Inherent Risk) x (1-(Management and Control Level /4)) + (0.25 x (Inherent Risk)

*Note: The **0.25** in the formula above represents 1 divided by the number of rating criteria being used. In this case, a 4-rating scale is being used. Therefore 1/4=0.25.*

RISK	ILLUSTRATIVE EXAMPLE
Master Planning and Sales Forecasting	Failure to properly forecast sales and inventory and prepare/execute a production plan that supports sales demand resulting in under or over production, inability to meet sales targets and financial losses due to working capital tied up in unsold inventory.
Likelihood	**4.0** (Expected to occur in given circumstances, >85% chance of occurrence)
Impact	**4** (Significant Impact given potential loss of sales >$35m and inability to execute strategy)
Management Control Score	**1.5** (Ineffective. Limited controls/risk management functions are in place. A high level of risk remains. High audit risk rating).
Inherent Risk	Impact x Likelihood – (4 x 4 = 16)
Residual Risk	(16) X (1 – (1.5/4)) + (0.25 x 16) ***Result = 10 + 4 = 14.00***
Risk Response	Very High - Improve

Step 6: Update Risk Master

Using the information obtained in the risk register, i.e. the risk, risk owner, and scores, update the Risk Master and prioritize risks based on residual risk. From the listing, create the LML Heat Map with the top 20 risks for presentation to the Management Team



A residual risk profile heat map helps management to understand the appropriate action associated with each risk. Possible management actions include:

- **Improve -** Areas of higher risk with a low level of control – these must be a key priority for control improvement activity.
- **Monitor risk** - Risks with low inherent exposure that also have a low level of control may be consciously accepted by Management, but the risk level must remain a focus of ongoing monitoring to identify increasing risk exposures.
- **Monitor controls -** Areas of high inherent risk where controls are asserted by Management to be adequate. Focus on continued monitoring of controls to ensure they continue to operate as designed and that risk is properly managed
- **Accept -** Areas of low inherent exposure with a high level of control are consciously accepted by the Company and in some instances, may generate opportunities to increase the effectiveness of processes and controls

Step 7: Validate and Prioritize Risks

A facilitation session should be held with the Management Team (and any other stakeholders invited to participate) to review the initial risk profiles prepared using feedback from ERA participants. The purpose of the session is to validate the findings with all participants so that an informed and generally accepted decision/rating can be assigned to rank the risks.

The primary outcome of the facilitation session is therefore to agree on the final risk ratings, prioritize risks and agree on action items to mitigate risks. Decisions and/or discussions taken at the facilitation session should be documented and used to update the risk profiles accordingly.

Step 8: Determine Action Items

Based on the classification of the risks above, action items should be developed to bring the risks closer to the 'accept' or 'monitor' (green to yellow) sections of the grid above. Other than avoiding risk entirely by terminating the activity, risk treatment options include:

- Reduce the likelihood of the risk occurring.
- Reduce the consequences of the risk occurring.
- Share/transfer the risk to another party e.g., contracts, insurance, outsourcing, joint ventures.

Action plans should be assigned to capable parties with the authority to effect change. Milestones and timelines should be documented and tracked for completion. Effective implementation should translate into reduced risk exposures on the heat map.

REVIEW AND ASSESSMENT OF THE ENTERPRISE RISK MANAGEMENT (ERM) POLICY

The Board will conduct a review and assessment of the ERM at least every 2 years in such manner as the Board deems fit.

.....
Lascelles Chin
Executive Chairman

.....
James E.D. Rawle
Director

DOCUMENT CONTROL

Version Number	*Reviewed by*	*Date Reviewed*	*Modifications*	*Approved by*	*Date Approved*