
I. Policy Introduction

The Board of Directors and Management of Lorenzo Shipping Corporation (LSC) consider risk management as a central or integral part of the organization’s strategic management. It is the process whereby LSC methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all business activities.

Risk Management is the culture, processes and structures that are directed towards realizing potential opportunities and managing adverse effects. It is a tool to help Management improve its decision-making process, minimize its losses, as well as maximize its profits. It offers a framework or process for effectively managing uncertainties, responding to risks, and exploring opportunities as they arise to ensure that value is created, protected, and enhanced.

The purpose of this risk management procedure is to provide all personnel of Lorenzo Shipping Corporation with the skills to apply consistent and comprehensive risk management methodology which includes how to identify, analyze, evaluate and control risks.

The risk management process contained in this manual follows the COSO Enterprise Risk Management Framework. It is a continuous and developing process which runs throughout the organization’s strategy and the implementation of that strategy. It should address methodically analyze all the risks surrounding the organization’s activities in the past and present so we can learn from it and protect the future.

II. Definition of Terms

Risk Management is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.

A risk is an uncertain event that will have a negative impact on the achievement of a business objective.

A control is a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives.

Inherent risk is a risk without regard to any management action or controls to alter or change its nature or state.

Residual risk is the remaining exposure after considering management action or control to reduce the impact or likelihood of the risk.

A risk appetite is the level of risk the organization is willing to take in pursuit of value or to achieve a desired level of return or growth – outcome. It can vary over time and from work to work area. The risk appetite must be articulated by the board and management and must be communicated across the organization.

Note: This policy is subject to final approval.
A risk tolerance is the acceptable levels of variation relative to the achievement of objective.

III. Objectives of Risk Management

Risk management is a responsibility of all LSC employees, with specific risk responsibilities being allocated to different groups and levels within the organization. It is important to have complete and current risk information available as this information assists management to make more informed decisions around both strategic direction and operational objectives.

Risk management is not a stand-alone discipline but requires integration with existing business processes such as business and budget planning, in order to provide us with the greatest benefits.

The objectives of a risk management framework are to:

- Provide a systematic approach to the early identification and management of risks;
- Provide consistent risk assessment criteria;
- Make available accurate and concise risk information that informs decision making including business direction;
- Adopt risk treatment strategies that are cost effective and efficient in reducing risk to an acceptable level; and
- Monitor and review risk levels to ensure that risk exposure remains within an acceptable level.

IV. Benefits of Risk Management

Application of a consistent and comprehensive risk management process will:

- Increase the likelihood of us achieving our strategic and business objectives;
- Encourage a high standard of accountability at all levels of the organization;
- Support more effective decision making through better understanding of risk exposures;
- Create an environment that enables us to deliver timely services and meet performance objectives in an efficient and cost effective manner;
- Safeguard our assets – human, property and reputation; and
- Meet compliance and governance requirements.

V. Roles and Responsibilities

Our ability to conduct effective risk management is dependent upon having an appropriate risk governance structure and well-defined roles and responsibilities.

Note: This policy is subject to final approval.
It is important for each LSC employee to be aware of his or her individual and collective risk management responsibilities because it is not merely about having a well-defined process but also about effecting the behavioral change in each of us so risk management is embedded in all organizational activities.

Set out below is LSC’s Risk Management Governance Structure. This structure illustrates that risk management is not the sole responsibility of one individual but rather occurs and is supported at all organizational levels.

**Risk Management Governance Structure**

**Board of Directors**

Among other things, the Board of Directors should:

- Establish the risk management governance structure including clear delineation of authority and responsibility over risk management at all levels across the organization;
- Set the risk appetite and risk tolerances of specific business activities or projects of the organization;
- Establish, communicate and commit to ethical values and code of conduct;
- Build competence and develop people within the organization;
- Establish risk management framework, policies, and procedures;
- Create risk awareness and training across the organization;
- Have oversight with knowledge and understanding of critical risks;
- Periodically review Risk Management Policy/Strategy Formulation and Implementation;

*Note: This policy is subject to final approval.*
- Define boundaries and limits that clearly exclude behaviors and actions that are off-strategy and unacceptable;
- Encourage and reward growth and innovation without creating unacceptable exposure to risk;
- Clarify, understand and manage risk appetite over the organization’s opportunity-seeking behavior in developing new products and new markets;
- Ensures that performance measures and targets do not encourage excessively risky behavior;
- Take an enterprise-wide view of risks, rather than a narrower unit or functional view, when selecting strategies to optimize risk and reward for the enterprise as a whole; and
- Obtain assurance that an effective internal controls and checks and balances are in place in high-risk areas.

**Risk Committee (RC)**

A board committee, either dedicated or one with other responsibilities, should assist the board to review risks, the risk management process and the significant risks facing the company.

The Risk Committee, is composed of the following members from the Board of Directors:

- Ms. Doris Magsaysay-Ho – Chairman
- Mr. Antony Louis L. Marden – Member
- Mr. Michael L. Escaler – Member

**President**

The President together with the Board of Directors creates an environment for risk management to operate effectively and, at the same time, ensuring that significant internal and external factors, including stakeholder interests, are considered in defining risk tolerance levels. The President act as:

- The comprehensive Risk Executive;
- The ultimate responsible for risk management priorities, tolerance, policies and strategies; and
- The final Enforcer on such matter.

**Risk Management Executive Committee (RMEC)**

The RMEC has the overall responsibility for risk management at the enterprise level, including:

- Strategic risk;
- Project risk; and
- Business or operational risks

*Note: This policy is subject to final approval.*
The RMEC shall appoint and mandate the members of the Risk Management Group and ensures that the risk management policies, strategies and methodologies are developed and carried out in an effective and efficient manner.

The RMEC is composed of the following company officers:

- Mr. Romualdo L. Bea, VP - Chief Financial Officer – Chairman
- Mr. Jay R. Olivarez, Liner Group Chief Operating Officer – Member
- Mr. Roland J. Portes, VP - Operations (Liner Group) – Member
- Mr. Edralin G. Manapsal, VP - Sales and Marketing (Liner Group) – Member

**Risk Management Group**

The Risk Management Group supports the RMEC in performing its responsibility in institutionalizing a sustainable risk management process within the organization.

- **Chairman:** Chief Risk Officer
- **Members:** Cluster Finance and Accounting Manager, Legal Manager, Compliance Officer, HR and Corporate Service Head, Technology Solutions Manager, Corporate Strategy Head, Branch Coordinating Manager and Internal Audit Manager.

The overall responsibility of the Risk Management Group includes the following:

- Review / validates / confirms risk issues generated by the Risk Management teams;
- Recommends RM tolerances to the RC;
- Evaluates measurement methodologies;
- Develop risk management policy, strategies, and initiatives for the approval of RC;
- Develop risk appetite strategy;
- Develops and implement systems, policies, and procedures for identification, collection, assessment and analysis, and mitigation of risks;
- Oversee the implementation of the risk management strategies and initiatives in compliance with established risk appetite;
- Assign owners of significant risk;
- Determine risk management tools and training requirements of the Risk Management Team; and
- Evaluates effectiveness of risk governance infrastructure for managing specific risks.

**Managers**

Operating and Line Managers are responsible for conducting a periodic risk assessment in their area of operations using the tools and methodology provided in this document. Among other things, they are responsible for the following:

- Supporting the risk culture of the organization;
- Identifying, communicating and managing risks in their area of operations;
- Preparing risk analysis worksheet (risk registers) on risks concerning their area of operations on a semi-annual basis; and

*Note: This policy is subject to final approval.*
• Managing risks on a day-to-day basis.

**Internal Audit**

The Internal Audit function will be responsible for providing assurance to RMEC and the Board of Directors on the appropriateness of the implementation of risk management strategies and the effectiveness of the risk management processes, methodologies and internal controls.

**External Auditors**

External audit, as part of their audit processes review controls that impact on the preparation of LSC’s Financial Statements.

**LSC Employees**

All LSC employees must comply with the company’s risk management policies and procedures. They are also responsible for identifying and reporting new emerging risks in their respective area of responsibilities to the appropriate level of authority.

**VI. Relationship with other processes**

Risk management is not a stand-alone discipline. In order to maximize risk management benefits and opportunities, it needs to be integrated with existing business processes.

Some of the key business processes with which risk alignment is necessary are:

• **Business planning (including budget)**

  Identifying risk during the business planning process allows us to set realistic delivery timelines for strategies/ activities or to choose to remove a strategy/ activity if the associated risks are too high or unmanageable. The impact of changing risk levels over the year can then be mapped to the relevant objective, enabling us to conduct more timely expectation management with key stakeholders.

• **Performance Management**

  All risk responsibilities, whether a general responsibility to use the risk management process or specific responsibilities such as risk ownership or implementation of risk treatments should be included within the relevant individuals’ performance plans (KPIs and KRAs).

• **Internal Audit**

*Note: This policy is subject to final approval.*
Internal Audit reviews the effectiveness of controls. Due to its limited resources, alignment between the Internal Audit function and that of the controls within the Risk Management process is critical. With risk management in place, the resources of Internal Audit will be optimized by aligning and focusing their reviews on business activities or processes that are most important to the organization or where the critical risks exist or could occur.

### VII. Key Process Steps

Risk management is a continual process that involves review and update of risk profiles for the enterprise as a whole and includes a review for each individual division in a “top-down” and a "bottom-up" approach to risk management.

This process is formally conducted across the entire organization on an annual basis during the corporate and business planning process.

Although this process is conducted across the entire organization on an annual basis, risk management is assessed throughout the year, in monthly reports, while making business decisions and when conducting day-to-day management.

The processes are:

1. Internal environment
2. Objective/Strategy setting
3. Event identification
4. Risk assessment
5. Risk response
6. Control activities
7. Communication and information
8. Monitoring

#### 1. Internal Environment

Internal Environment reflects the philosophy or attitude of the whole organization through directives from the Board. This can be achieved through but not limited to the following activities:

- **Risk Policies**
  
  The Board reviews and amends the risk management governance structure including clear delineation of authority and responsibility over risk management at all levels across the organization if necessary;

  The Board sets changes to risk appetite and risk tolerances of specific business activities or projects of the organization.

- **Risk Appetite and Tolerances**

*Note: This policy is subject to final approval.*
The LSC strategic planning process must take the organization’s risk appetite policies into account (for example debt to equity ratio limits).

c. Risk Management Capabilities

Building, establishing, and creating competence, risk management framework, policies and procedures, and awareness respectively across the organization.

2. Setting Strategies and Establishing Clear Objectives

Objectives that support and are aligned with our organization’s mission and are consistent with risk appetite must be established before management can identify potential events affecting their achievement.

3. Event Identification

After a clear understanding of the vision, mission, objectives and strategies, both internal and external inherent risks events and opportunities must be identified.

For common risk language, the risk assessment team should use the Risk Business Model table below during their event identification process.

As shown in the above table, risks are categorized in to three namely:

- **Environment** - Arises when there are external forces that could affect the viability of the firm’s business model, including fundamentals that drive the overall objectives and strategies that define the model. These risks are outside management’s ability to control.

- **Process Risks** - The risks that business processes within the organization are not clearly defined, are poorly aligned with business objectives and strategies, do not satisfy customer needs dilute shareholders value, or expose assets & resources to misappropriation or misuse.

*Note: This policy is subject to final approval.*
• **Information for Decision Making Risks** – The risks that information used to support strategic, operational and financial decisions is not relevant or reliable. This risk relates to the usability and timeliness of information that is either created or summarized by processes and application systems or a failure to understand information needs.

A risk definition or glossary for each risk of categories under each major risk classification are provided in Appendix A of this Manual for easy reference.

4. **Risk Assessment**

Once the *Inherent Risks* are identified, each potential risk is analysed based on an assessment of its consequence and likelihood.

*Consequence* is measured according to the magnitude of a loss, if the risk comes to pass. How bad are the scenarios? How significant is the potential loss? How damaging is this to the image of the organization? Does this warrant management interest or attention?

Below is a sample matrix for consequence:

<table>
<thead>
<tr>
<th>CONSEQUENCE (Impact/Severity)</th>
<th>NUM VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Material</td>
<td>5</td>
<td>- &gt;Php ___ M impact on profitability; or&lt;br&gt; - Loss of key alliances; or&lt;br&gt; - Sustained serious loss in market share; or&lt;br&gt; - Immediate Board and Sr. Management attention required</td>
</tr>
<tr>
<td>Significant</td>
<td>3</td>
<td>- &gt;Php ___ M to &lt;Php ___ M or x% impact on profitability; or&lt;br&gt; - Key alliances are threatened; or&lt;br&gt; - Serious diminution in brand value &amp; market share with adverse publicity; or&lt;br&gt; - Events and problems require Board and Sr. Management attention</td>
</tr>
<tr>
<td>Insignificant</td>
<td>1</td>
<td>- &lt;Php ___ M impact on profitability; or&lt;br&gt; - No potential impact on market share; or&lt;br&gt; - No impact on brand value; or&lt;br&gt; - Issues would be delegated to Managers and staff to resolve.</td>
</tr>
</tbody>
</table>

*Likelihood* is measured according to the probability of the occurrence of the event……in other words, its frequency. Will this really happen? Has this happened in the past? This could be based on your experiences, history of previous events or relevant knowledge and expertise.

Below is a sample matrix for likelihood:

*Note: This policy is subject to final approval.*
LIKELIHOOD (Probability/Frequency) | NUM VALUE | DESCRIPTION
--- | --- | ---
Highly Probable | 5 | - Event is expected / certain to occur sometime in the next 12 months; or - Has occurred many times in the past year.
Reasonably Possible | 3 | - Event will probably occur or is highly likely to happen in the future; or - Has occurred in the past.
Remote | 1 | - Event may only occur or is highly unlikely to occur in exceptional circumstances; or - Has occurred once beyond 5 years.

After each potential risk event are measured according to its likelihood and consequence, those involve in risk assessment will need to plot those risks into the Risk Heat Map as shown below:

By plotting the risks identified into the Risk Heat Map taking into consideration its consequence and likelihood, we can now visualize risks in relation to each other and can be used as a basis for assessing and addressing risks in accordance to their potential impact on the business strategy.

Note: This policy is subject to final approval.
Those risk falling under the red colored grids are your *Critical risks*, the yellow ones are the *High* risks and those that are in the green colored grids are the *Low risks*.

Critical risks are classified as primary risks and are rated “High” priority because they threaten the achievement of business objectives. High risks are second priority next to primary risks and Low risks are both unlikely to occur and its impact is not that significant.

Why do we need to prioritize our risks?
- To determine which risks are more important or critical to the organization
- To determine which risks deserve more attention; and
- Within an audit perspective, to devote limited audit resources according to priority.

After risks have been identified, measured and prioritized, the next step is to consider risk response options that could bring the level of the risk impact to a desired level acceptable to Management and the Board.

5. *Risk Response*

Risk response involves examining possible treatment options to determine the most appropriate action for managing a risk. Management actions or risk responses are required where the current controls are not managing the risk within defined tolerance levels. Response could involve improving existing controls and implementing additional controls.

Possible risk treatment options include:

- **Take** – do nothing, retain the risk and accept impact of the risk (ex. Self-insure);
- **Transfer** – transfer risk ownership and liability to a 3rd party (ex. insurance, outsourcing, hedging, etc.);
- **Terminate** - change business process or objective so as to avoid the risk (e.g. eliminate, prohibit, divest, etc.); and
- **Treat** - undertake actions aimed at reducing the cause and impact of the risk (e.g. process or control improvement, re-organization, re-design, etc.)

When determining the preferred risk response option, consideration should be given to the cost of the treatment as compared to the likely risk reduction that will result (cost benefit analysis).

On selecting the preferred treatment option, the following should occur:

- The cost of any actions should be incorporated into the relevant budget planning process;
- A responsible person should be identified for delivery of the action, with this expectation being communicated to them;

*Note: This policy is subject to final approval.*
• A realistic due date should be set; and
• Performance measures should be determined.

Risk response also involves:

• Identifying controls currently in place to manage the risk by either reducing the consequence or likelihood of the risk;
• Assessing the effectiveness of current controls;
• Identifying the likelihood of the risk occurring; and
• Identifying the potential consequence or impact that would result if the risk was to occur.

6. Control Activities

When evaluating the effectiveness of current controls, the factors to consider include consistency of application, understanding of control content and documentation of controls where appropriate. Controls are aimed at bringing the risk within an acceptable level. The evaluation of current controls can occur through several different processes including:

• Control self-assessment;
• Internal Audit reviewing the effectiveness of controls; and
• External Audit reviewing the effectiveness of controls.

The consequence and likelihood ratings, as identified after consideration of current controls, are combined to determine the overall risk level or residual risk.

Risk evaluation involves considering the risk’s overall risk level. This allows determination of whether further risk treatment actions are required to bring the risk within a level acceptable.

The output of the risk evaluation phase is a prioritized list of risks.

There may be times when the action required will differ from that identified above; however where this is the case, the Chief Executive Officer must approve deviation from the above action.

7. Communication and Information

Risk management reporting is a key element of the ‘Monitor and Review’ phase of the risk management process, and needs to occur at each step of the process. This risk management reporting process supports a formalized, structured and comprehensive approach of the company to monitor and review of its risks, thereby enhancing its risk management process.

8. Monitoring and Reviewing Risk

Risk information requires regular monitoring and review to ensure currency. The environment in which we operate is constantly changing and so therefore are our risks. If risk information is inaccurate, we may make poor decisions that could otherwise have been avoided.

Note: This policy is subject to final approval.
Therefore Risk Owners and Risk Management Team have key risk and control review and update responsibilities to ensure continued currency of information pertaining to their particular risks. In addition, on an annual basis, the entire risk register will be reviewed, with review participation of Senior Management and the board as necessary.

It is also important for the effectiveness of the risk management framework to be monitored and reviewed. This framework drives the extent to which risks will be adequately managed throughout the organization. Monitoring implementation of the Risk Management Strategy is one available monitoring mechanism.

In addition, the risk management framework itself will be reviewed annually, with results being reported to the RMC and the Board. As risk management developments are constantly occurring, this review mechanism will provide us with information on current risk management developments, facilitating us making continuous risk management improvements.

**VIII. The Risk Register**

The Risk Register contains all the risks identified and summarizes or documents the results of the assessment performed including management actions to be undertaken to further mitigate the risks to an acceptable level. It also include information as to whom (individual or unit) specific risks are assigned and responsible for its mitigation. Information that should be included in the detailed risk register are as follows:

- Area, unit, process, activity or project with which the risk is associated
- Objective/s or goal/s to be achieved
- Risk description
- Business Risk Category
- Business Objective Category
- Risk reference number
- Assessment score for likelihood (5, 3, 1)
- Assessment score for consequence (5, 3, 1)
- Overall risk assessment (H, M, L)
- Value at risk or significance
- Existing controls that mitigate the risks
- Residual risk after existing controls
- Future or action plan to further improve mitigation controls including timeline, responsible person, and status

This detailed risk register is accomplished or produced during the annual risk review process unless otherwise specifically requested by the Board, RC, or RMEC.
## Risk Register Template

<table>
<thead>
<tr>
<th>Strategies, Plans &amp; Programs, Project, Core Process &amp; Activity</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
<th>N</th>
<th>O</th>
<th>P</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate Goal and Objective</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Category (Environment, Process, Information Risk)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Objective Category (Strategic, Operations, Reporting, Compliance)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specific Risk Event/Opportunity (Inherent Risk)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Ref. Nbr.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likelihood</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Impact</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assessment (B, M, U)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Value at Risk or Significance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Existing Risk Mitigation Controls/Strategy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Residual Risk/Remaining Risk after Controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Resolution Plan/Risk Mitigation Strategy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timeline/Status</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Owner/Person Responsible/Owner of Risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: Columns C & O are optional.

## Risk Status Reporting

<table>
<thead>
<tr>
<th>Risk Ref. No.</th>
<th>Specific Risk Event</th>
<th>Risk Category</th>
<th>Before Controls</th>
<th>After Controls</th>
<th>Trend</th>
<th>Control Improvement</th>
<th>Responsible Officer</th>
<th>Status</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS-001</td>
<td>Improper disposal of used oil and lube</td>
<td>Process/Operations Environment Risk</td>
<td>☢</td>
<td>☢</td>
<td>☢</td>
<td>Establish policies and procedures for used oil and lube disposal</td>
<td>VP - HSSE</td>
<td>☢</td>
<td>90% Complete. Estimated made due date - July 31, 2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Internal Audit to review compliance annually</td>
<td>CAE</td>
<td>☢</td>
<td>Audit results to be submitted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Procurement of proper container for used oil and lube and relocation of temporary storage facility</td>
<td>Mgr - Purchasing</td>
<td>☢</td>
<td>Ongoing reviewer conducted</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Overall Assessment</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Not started</td>
</tr>
<tr>
<td>Moderate</td>
<td>Ongoing</td>
</tr>
<tr>
<td>Low</td>
<td>Completed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trend</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Increasing</td>
<td>☢</td>
</tr>
<tr>
<td>Stable</td>
<td>☢</td>
</tr>
<tr>
<td>Decreasing</td>
<td>☢</td>
</tr>
</tbody>
</table>

Note: This policy is subject to final approval.
Appendix - Definition of Business Risks

I. Environment Risk

Environment risk arises when there are external forces that can affect a company's performance, or make its choices regarding its strategies, operations, customer and supplier relationships, organizational structure or financing obsolete or ineffective. These forces are outside management's ability to control.

A. Competitor Risk

Major competitors or new entrants to the market take actions to establish and sustain competitive advantage over the company or even threaten its ability to survive.

B. Customer Wants Risk

The company is not aware that customer needs and wants change. Such needs and wants may apply to desired quality, willingness to pay and/or speed of execution.

C. Technological Innovation Risk

The organization is not leveraging advancements in technology in its business model to achieve or sustain competitive advantage or is exposed to the actions of competitors or substitutes that do leverage technology to attain superior quality, cost and/or time performance in their products, services, and processes.

D. Sensitivity Risk

Sensitivity risk results when management commits the company's resources and expected cash flows from future operations to such an extent that it reduces the company's tolerance for (or ability to withstand) changes in environmental forces that are totally beyond its control.

E. Shareholder Expectations Risk

The risk of failing to manage shareholder expectations, resulting in a decline in investor confidence that may impair the company's ability to efficiently raise capital and reduce stock evaluations over time.

F. Capital Availability Risk

The company does not have efficient access to the capital it needs to fuel its growth, execute its strategies, and generate future financial returns.

G. Sovereign/Political Risk

The risk of adverse consequences through political actions in a country in which a company has made significant investments (a major project, for example), is dependent on a significant volume of business or has entered into an agreement with a counter party subject to the laws of that country.

H. Legal Risk

Note: This policy is subject to final approval.
The risk that a company's transactions, contractual agreements and specific strategies and activities are not enforceable under applicable law.

I. Regulatory Risk

Changes in regulations and actions by national or local regulators can result in increased competitive pressures and significantly affect a company's ability to efficiently conduct business.

J. Industry Risk

The risk that the industry will lose its attractiveness due to changes in the key factors for competitive success within the industry, capabilities of existing and potential competitors, and company's strengths and weaknesses relative to competitors.

K. Financial Markets Risk

Financial markets risk is defined as exposure to changes in the earnings capacity or economic value of the firm as a result of changes in financial market variables (e.g., currency rates). These changes affect income, expense or balance sheet values.

L. Catastrophic Loss Risk

The inability to sustain operations, provide essential products and services, or recover operating costs as a result of a major disaster.

II. Process Risk

The risk that business processes are not clearly defined, are poorly aligned with business objectives and strategies, do not satisfy customer needs, dilute shareholder wealth, or expose assets to misappropriation or misuse.

A. Governance Risk

The risk that the organization's governance processes do not comply with legal requirements or stakeholder expectations and that the board of directors fails to provide adequate monitoring and oversight of executive management activities.

1. Organizational Culture Risk

The organization's culture does not encourage managers to realistically portray the potential outcomes of transactions, deals, investments and projects and understand and portray the full picture for decision makers. The organization experiences dysfunctional behavior because managers are either risk averse or incented to take risks beyond the organization's risk appetite.

2. Ethical Behavior Risk

The organization, through its actions or inaction, demonstrates that it is not committed to ethical and responsible business behavior.

3. Board Effectiveness Risk

Note: This policy is subject to final approval.
The board does not constructively engage management and provide anticipatory, proactive and interactive oversight of the company's activities and affairs, with integrity, vision, common sense and unquestioned independence.

4. Succession Planning Risk
Leadership talent within the organization is not sufficiently developed to provide for orderly succession in the future.

B. Reputation Risk
The risk of loss of brand image such that the company will be unable to operate in the marketplace.

1. Image and Branding Risk
The risk that a company may lose customers, key employees or its ability to compete, due to perceptions that it does not deal fairly with customers, suppliers and stakeholders, or know how to manage its business.

2. Stakeholder Relations Risk
A decline in investor confidence may impair a company's ability to efficiently raise capital. The company will not have the same efficient access as competitors to the capital it needs to fuel its growth, execute its strategies, and generate future financial returns.

C. Operations Risk
The risk that operations are inefficient and ineffective in satisfying customers and achieving the company's quality cost and time objectives.

1. Customer Satisfaction Risk
The company's processes do not consistently meet or exceed customer expectations due to a lack of focus on the customer.

2. Human Resources Risk
The personnel responsible for managing and controlling an organization or a business process do not possess the requisite knowledge, skills and experience needed to ensure that critical business objectives are achieved and significant business risks are reduced to an acceptable level.

3. Knowledge Capital Risk
Processes for capturing and institutionalizing learning across the organization are either nonexistent or ineffective, resulting in slow response time, high costs, repeated mistakes, slow competence development, constraints on growth and unmotivated employees.

4. Product Development Risk
The productivity of the product development process is significantly less than more innovative competitors who are able to achieve higher productivity through a stronger customer focus, concentrating focused resources and faster cycle time.

Note: This policy is subject to final approval.
5. Efficiency Risk
The process is inefficient in satisfying valid customer requirements resulting in higher than competitive costs.

6. Capacity Risk
The effective productive capacity of the plant is not fully utilized, resulting in spreading fixed costs over fewer units and creating higher unit costs and lower unit margins or the capacity does not fulfill customer needs resulting in a loss of business.

7. Scalability Risk
The inability to operate differently and more efficiently at larger volumes or amortize costs over greater sales volume, resulting in diseconomies of scale that threaten the firm’s ability to generate competitive profit margins.

8. Performance Gap Risk
A business process does not perform at a world-class level because the practices designed into the process are inferior.

9. Cycle Time Risk
Elapsed time between the start and completion of a business process (or activity within a process) is too long because of redundant, unnecessary and irrelevant steps.

10. Sourcing Risk
The fewer the alternative sources of energy, metals and other key commodities and raw materials used in a company's operations, the greater the risks of shortages and higher costs. These risks can significantly affect the company's capability to provide competitively priced products and services to customers at the time they are wanted.

11. Channel Effectiveness Risk
Poorly performing or positioned distribution channels threaten the organization's capacity to access current and potential customers/end users effectively and efficiently.

12. Partnering Risk
Inefficient or ineffective alliance, joint venture, affiliate and other external relationships affect the organization’s capability to compete. These uncertainties arise due to choosing the wrong partner, poor execution, receiving more value than is given (ultimately resulting in loss of a partner) and failing to capitalize on partnering opportunities.

13. Compliance Risk
As a result of a flaw in design or operation or due to human error, oversight or indifference, the company's processes do not meet customer requirements the first time or do not comply with prescribed procedures and policies. Compliance risk can also result in failure to conform with laws and regulations at the international, country, state and local level that apply to a business process.

Note: This policy is subject to final approval.
14. Business Interruption Risk

The company's capability to continue critical operations and processes may be highly dependent on availability of certain raw materials, information technologies, skilled labor and other resources.

15. Product/Service Failure Risk

The company's operations create risk of customers receiving faulty or nonperforming products or services.

16. Environmental Risk

Environmental risks expose companies to potentially enormous liabilities. The exposure is twofold -- (1) liability to third parties for bodily injury or property damage caused by the pollution, and (2) liability to governments or third parties for the cost of removing pollutants plus severe punitive damages.

17. Health and Safety Risk

These risks expose a company to potentially significant workers' compensation liabilities, financial loss, and negative publicity. Firms and their managers could find themselves criminally liable for failure to provide a safe working environment for their employees.

18. Trademark/Brand Erosion Risk

The risk that a trademark or brand will lose its value. A trademark is a word, symbol or device -- or any combination of these -- that identifies a product or service and distinguishes that product or service from the products or services of competitors.

D. Empowerment Risk

The risk that managers and employees are not properly lead, do not know what to do (or how to do it) when they need to do it, exceed the boundaries of their defined authorities, do not have the resources, training and tools necessary to make effective decisions or are given incentives to do the wrong thing.

1. Leadership Risk

The risk that the people responsible for the important business processes do not or cannot provide the leadership, vision, and support necessary to help employees be effective and successful in their jobs.

2. Authority/Limit Risk

The risk that people either make decisions or take actions that are not within their explicit responsibility or control or fail to take responsibility for those things for which they are accountable. Failure to establish or enforce limits on personnel actions may cause employees to commit unauthorized, illegal or unethical acts or assume unauthorized or unacceptable business risks.

3. Outsourcing Risk

Note: This policy is subject to final approval.
Outside service providers do not act within their defined limits of authority and do not perform in a manner consistent with the values, strategies and objectives of the company.

4. Performance Incentives Risk

Unrealistic, subjective or unclear performance measures may cause managers and employees to act in a manner that is inconsistent with the company’s business objectives, strategies, ethical standards and prudent business practice.

5. Change Readiness Risk

The people within the organization are unable to implement process and product/service improvements quickly enough to keep pace with changes in the marketplace.

6. Communications Risk

Communication channels (top-down and bottom-up or cross-functional) within the organization are ineffective and result in messages that are inconsistent with authorized responsibilities or established measures.

E. Information Technology Risk

The risk that the information technologies used in the business are not efficiently and effectively supporting the current and future needs of the business or threaten the company’s ability to sustain the operation of critical business processes.

1. Integrity Risk

This risk encompasses all of the risks associated with the authorization, completeness, and accuracy of transactions as they are entered into, processed by, summarized by and reported on by the various application systems deployed by an organization.

2. Access Risk

Access risk includes the risk that access to information (data or programs) or systems will be inappropriately granted or refused. It encompasses the risks of improper segregation of duties, risks associated with the integrity of data and databases and risks associated with information confidentiality.

3. Availability Risk

The risk that information will not be available when needed. This includes risks such as loss of communications (e.g., cut cables, telephone system outage, satellite loss and etc.), loss of basic processing capability (e.g., fire, flood, electrical outage) and operational difficulties (e.g., disk drive breakdown, operator errors).

4. Infrastructure Risk

The risk that the organization does not have an effective information technology infrastructure (e.g., hardware, networks, software, people and processes) to effectively support the current and future needs of the business in an efficient, cost-effective and well-controlled fashion.

Note: This policy is subject to final approval.
F. Integrity Risk

The risk of management fraud, employee fraud, and illegal and unauthorized acts, any or all of which could lead to reputation degradation in the marketplace or even financial loss.

1. Management Fraud Risk

Management issues misleading financial statements with intent to deceive the investing public and the external auditor or engages in bribes, kickbacks, influence payments and other schemes for the benefit of the company.

2. Employee Fraud and Third Party Fraud Risk

Fraudulent activities perpetrated by employees, customers, suppliers, agents, brokers or third-party administrators against the organization for personal gain expose the organization to financial loss.

3. Illegal Acts Risk

Managers and employees individually or in collusion commit illegal acts, placing the company, its directors and officers at risk to the consequences of their actions.

4. Unauthorized Use Risk

The company’s employees (or others) use its physical and financial assets for unauthorized or unethical purposes.

G. Financial Risk

Financial risk can occur if the company fails to provide adequate liquidity to meet the firm’s obligations or manages financial risks in a manner that is inconsistent with the firm’s business objectives. Its severity depends on a number of factors, which include the firm’s size, industry, financial position (e.g. public/private, leverage, free cash flow to equity, etc.), and the direction of the market as a whole.

1. Price Risk

The exposure of earnings or net worth to changes in market factors (e.g., interest rates, currency rates), which affect income, expense or balance sheet values.

a. Interest Rate Risk

The risk that interest rates deviate from their expected value resulting in lower-than-expected investment yields, higher-than-expected borrowing or product costs, or deterioration of the firm’s competitive position in its industry.

b. Currency Risk

The exposure to fluctuations in exchange rates may arise as a result of business activity in foreign markets and investment in securities, which are issued by overseas entities or are denominated in a foreign currency.

c. Equity Risk

Note: This policy is subject to final approval.
The exposure to fluctuations in the income stream and/or value of equity ownership in an incorporated entity.

d. Commodity Risk

This can be a financial market risk if a company chooses an investment as part of a diversification strategy for managing investment risk. From the industrial perspective, commodity risk is the exposure to fluctuations in prices of commodity-based materials or products (e.g., gold, energy, copper, coffee and etc.).

e. Financial Instrument Risk

Financial market risk can vary depending upon the particular segment of the market to which the holder of a financial instrument is exposed, or the way in which the exposure is structured.

2. Liquidity Risk

The exposure to loss as a result of the inability to meet cash flow obligations in a timely and cost-effective manner. Liquidity risk often arises as a result of an investment portfolio with a cash flow and/or maturity profile, which differs from the underlying cash flows dictated by the company’s operating requirements and other obligations.

a. Cash Flow Risk

Actual losses incurred as a result of the inability to fund the operational or financial obligations of the business.

b. Opportunity Cost Risk

The use of funds in a manner that leads to the loss of economic value, including time value losses, transaction costs due to inappropriate or inefficient management of cash flows and other causes of loss of value.

c. Concentration Risk

Exposure to loss as a result of the inability to access cash in a timely manner due to the inability to liquidate exposures without moving the market, unusual market conditions, use of “proprietary” financial products, or excessive reliance on a small number of funding sources.

3. Credit Risk

The exposure to actual loss or opportunity cost as a result of default (or other failure to perform) by an economic or legal entity (the debtor) with which the company does business.

a. Default Risk

A counterparty will be unable to fulfill its obligations.

b. Concentration Risk

Inappropriate emphasis of sales volume or revenues on a single customer, industry sector, or other economic segment leads to exposure to excessive loss.

c. Settlement Risk

Note: This policy is subject to final approval.
In financial terms, this risk arises when financial counterparties effect their payments to each other at different times or in different locations. In a non-financial context, settlement risk describes the risk of unexpected costs and/or administrative inconvenience associated with the failure to deliver payment in the right place at the right time.

d. Collateral Risk

This is the risk that the value of an asset provided as collateral for a loan, receivable, or commitment to perform may be partially or totally lost.

III. Information for Decision-Making Risk

The risk that information used to support strategic, operational and financial decisions is not relevant or reliable. This risk relates to the usability and timeliness of information that is either created or summarized by processes and application systems or a failure to understand information needs.

A. Operational Risk

1. Budget and Planning Risk

Budgets and business plans are not realistic, based on appropriate assumptions, based on cost drivers and performance measures, accepted by key managers, or used as a monitoring tool.

2. Product/Service Pricing Risk

The company's price is more than customers are willing to pay or does not cover production and distribution costs.

3. Contract Commitment Risk

The company does not have information that effectively tracks contractual commitments outstanding at a point in time, so that the financial implications of decisions to enter into incremental commitments can be appropriately considered by decision makers.

4. Measurement (Operations) Risk

Process performance measures do not provide a reliable portrayal of operating performance and do not accurately reflect reality. The measures do not provide relevant information for decision making because they are not informative, understandable, believable, actionable, or indicators of change.

5. Alignment Risk

The objectives and performance measures of the company's business processes are not aligned with its overall business objectives and strategies. The objectives and measures do not focus people on the right things and lead to conflicting, uncoordinated activities.

6. Accounting Information Risk

Note: This policy is subject to final approval.
Financial accounting information used to manage business processes is not properly integrated with nonfinancial information focused on customer satisfaction, measuring quality, reducing cycle time and increasing efficiency. The result is a myopic, short-term fixation on manipulating the outputs of business processes to achieve financial targets, rather than fulfilling customer expectations by controlling and improving processes.

**B. Public Reporting**

1. **Financial Reporting Evaluation Risk**

   Financial reports issued to existing and prospective investors and lenders include material misstatements or omit material facts, making them misleading.

2. **Internal Control Evaluation Risk**

   Failure to accumulate sufficient relevant and reliable information to assess the design and operating effectiveness of internal control over financial reporting, resulting in inaccurate assertions by management in the internal control report.

3. **Executive Certification Risk**

   Failure to accumulate sufficient, relevant and reliable information to assess the design and operating effectiveness of disclosure controls and procedures, resulting in material information not being disclosed timely to certifying officers and in public reports.

4. **Taxation Risk**

   Significant transactions of the company have adverse tax consequences that could have been avoided had they been structured differently. Failure to comply with all tax regulations (e.g. payment and filing requirements) creates risks.

5. **Pension Fund Risk**

   Pension funds are not actuarially sound, e.g., they are insufficient to satisfy benefit obligations defined by the plan.

6. **Regulatory Reporting Risk**

   Reports of operating and financial information required by regulatory agencies are incomplete, inaccurate, or untimely, exposing the company to fines, penalties and sanctions.

**C. Strategic Risk**

1. **Environmental Scan Risk**

   The failure to monitor and stay in touch with a rapidly changing environment resulting in obsolete business strategies.

2. **Business Model Risk**

   The organization has an obsolete business model and doesn't recognize it and/or lacks the information needed to make an up-to-date assessment of its current model and build a compelling business case for modifying that model on a timely basis.

3. **Business Portfolio Risk**

*Note: This policy is subject to final approval.*
The risk that a firm will not maximize business performance by effectively prioritizing its products or balancing its businesses in a strategic context.

4. Investment Valuation /Evaluation Risk

Management does not have sufficient financial information to make informed short-term and long-term investment decisions and link the risks accepted to the capital at risk. Management and key decision-makers are unable to reliably measure the value of a specific business or any of its significant segments in a strategic context.

5. Organization Structure Risk

The company's organizational structure does not support change or the company's business strategies.

6. Measurement (Strategy) Risk

Occurs when overall organizational performance measures focus primarily on near-term financial results or are not consistent with and do not support business strategies.

7. Resource Allocation Risk

The company's resource allocation process does not establish and sustain competitive advantage or maximize returns for shareholders.

8. Planning Risk  The company's business strategies are not driven by creative and intuitive input or based on current assumptions about the external environment resulting in strategies that are out-of-date and unfocused.

9. Life Cycle Risk

An organization's approach to managing the movement of its product lines and evolution of its industry along the life cycle (e.g., start-up, growth, maturity and decline) threatens the ultimate success of its business strategies.

Note: This policy is subject to final approval.