SOLID GROUP INC.
ENTERPRISE RISK MANAGEMENT POLICY

SECTION 1. PURPOSE

This Policy establishes the standards, processes and accountability structure to identify, assess, prioritize and manage key risk exposures across Solid Group Inc. and its Subsidiaries ("The Group"). It will enable the executive and managers at all levels to systematically evaluate implications of decisions and actions to the highest priority goals and objectives, and effectively manage a broad array of risks in an informed and strategic manner to within an acceptable tolerance level.

SECTION 2. SCOPE

This Policy applies to all plans, activities, business processes, policies, procedures, individuals, entities and property that comprise The Group.

SECTION 3. POLICY STATEMENT

The Group engages in a wide range of business activities, all of which give rise to some level of risks. It is the policy of the Group to:

1. Embed risk management into the culture and operations of the Group
2. Integrate ERM into strategic planning, activity planning, performance management and resource allocation decisions
3. Manage risk and leverage opportunities in accordance with best practices
4. Regularly re-assess the Group's risk profile and the effectiveness of risk response in the context of the various strategic plans
5. Anticipate and respond to changing social, technological, environmental, government and market requirements.

SECTION 4. DEFINITION OF TERMS

Enterprise Risk Management – **"ERM"** is the process of identifying, analyzing and managing strategic risks. It provides the methodology for integrating risk into the strategic planning and resource allocations processes at the strategic level.

Executive Management – Are the executive officers (i.e., President & CEO, and Senior Vice Presidents) of the holding/mother company of the Group.

Local Management – Compose of the Presidents, Vice Presidents, General/Operating Managers or Company Head of the member companies of the Group.

Risk – is the chance that an event, trend or course of action will have either a positive or negative effect on an organizations ability to meet its strategic or operational objectives.

Risk Analysis – is the process of determining the likelihood of a particular event, trend or course of action occurring and the impact on operational or strategic objectives if it does.

Risk Owners – are middle managers or supervisors typically responsible for one or more functions, and are directly responsible to implement risk treatments as directed by local management.

Risk Register – a list of identified enterprise risks which documents the risk analysis, risks scores, risk treatments, direction, result of risk treatments and status of each risk.

Risk Tolerance – sometimes known as risk appetite, is the level of risks the organization is willing to accept for any event, trend or course of action. Risks tolerance will vary depending on the potential effect of the risk on the organization's operational or strategic objectives.

Risk Treatment – sometimes known as risk control, is the measures used to modify the risk to fall within the organization's risk tolerance for that risk. Options include accept, mitigate, transfer, avoid or exploit the event, trend or course of actions.

SECTION 5. BENEFITS

After successful implementation of ERM, The Group expects the following benefits:

a. More efficient use of capital and resources
b. Reduced likelihood of operational loss
c. Lower compliance costs
d. Earlier detection of illegal activities
e. Fewer surprises
f. Focus on lower cost prevention rather than higher cost resolution strategies
g. Cost savings by using risk information to streamline and improve processes
h. Increased awareness and integrated view of risks (existing and emerging)
i. Systematic, repeatable approach to mitigate risks and identify opportunities
j. Clearer, better informed decision

By being informed, the Board and Executive Management can be proactive in responding to the significant risks and opportunities that The Group experiences. ERM helps identify strategically significant high priority risk issues for the Board's attention. Through a comprehensive risk identification and assessment process, the organization can identify who owns the risks and how best to respond to the risk. This ensures that the most appropriate and optimum level of resources is assigned to areas of greatest risk. ERM helps identify opportunities as well as identifying risks. To be effective and not created additional overhead, ERM should be integrated into existing processes within the organization to support such

activities as strategic planning, business-planning, compliance monitoring, performance measurement, policies and procedures formulation, and process re-engineering.

SECTION 6. ROLES AND RESPONSIBILITIES

The Group established the framework of responsibilities which is consistent with the following generally recognized basic principles of sound risk management practice:

a. The development of risk management processes that provide for risk and exposure monitoring;
b. The embedding or integration of risks management into all activities as an integral part of the enterprise's business activities; and
c. The development of comprehensive internal control and assurance processes linked to key risks.

6.1 Oversight by the Board

The Group's Board will undertake oversight of the program, including:

- The oversight of both risk and the implementation of sound risk management systems;
- Responsibility for approving the Policy, reviewing the effectiveness of the risk management processes and articulating the risk appetite of The Group;
- Responsibility for approving policies on governance, risk and compliance and seeking regular assurance from Executive and Local Management, Audit Services and/or the External Auditors that enables the Board to ensure the system of internal control is operating effectively; and
- Delegating responsibility to Executive and Local Management in managing the program.

6.2 The Executive and Local Management

The roles and responsibilities of The Group's Management include:

- Risk management planning and oversight under the leadership of the CEO;
- Ensuring sound risk management systems and practices are established and maintained to give effect to this Policy and the risk appetite statements approved by the Board;
- Ensuring the accurate, timely and consistent flow of risk management information to the Board;
- Designing and implementing appropriate risk management processes and controls, some of which will be enterprise-wide and some of which will be business/project-specific; and
- Establishing a sound risk aware culture throughout the enterprise.

6.3 The Risk Management Committee

The Risk Management Committee ("RMC") is appointed by the Board to assist them to discharge their responsibilities for risk management. In discharging its governance responsibilities relating to risk management, the RMC should:

- Review and recommend for the approval of the risk management policy, risk management strategy, risk management implementation plan, organization's risk tolerance, and risk identification and assessment methodologies.
- Evaluate the extent and effectiveness of integration of risk management within the organization;
- Assess implementation of the risk management policy and strategy (including plan);
- Evaluate the effectiveness of the mitigating strategies implemented to address the material risks of the organization;
- Review the material findings and recommendations by assurance providers on the system of risk management and monitor the implementation of such recommendations;
- Develop its own key performance indicators for approval by the Board;
- Interact with the Audit Committee to share information relating to material risks of the organization; and
- Provide timely and useful reports to the Board on the state of risk management, together with accompanying recommendations to address any deficiencies identified.

6.4 The Audit Committee

The Audit Committee is an independent committee responsible for oversight of the organization's control, governance and risk management. Its responsibilities should include;

- Reviewing and recommending disclosures on matters of risk in the annual financial statements;
- Reviewing and recommending disclosures on matters of risk and risk management in the annual report;
- Providing regular feedback to the Board on the adequacy and effectiveness of risk management in the organization, including recommendations for improvement;
- Ensuring that the internal and external audit plans are aligned to the risk profile of the organization;
- Satisfying itself that it has appropriately address the following are:
    - Financial reporting risks, including the risks of fraud;
    - Internal controls; and
    - IT risks
- Evaluating the effectiveness of Internal Audit in its responsibilities for risk management.

6.5 Group Internal Audit

Group Internal Audit is an independent appraisal function established to provide assurance to the Board, and the Audit Committee about the adequacy and effectiveness of existing internal controls.

More specifically, Group Internal Audit is responsible for:

a) Developing and implementing an annual audit plan having regard to The Group's materials risks;
b) Reviewing the effectiveness of The Group's risk management policy and risk management processes; and
c) Notifying the Risk Management Committee and Audit Committee of new and emerging risks identified in the course of implementing the audit plan and, where necessary, modifying the audit plan to take account of the impact of new risks.

6.6 Employees

Employees are responsible for integrating risk management into their day-to-day activities. Some high level responsibilities include:

- Applying the risk management process in their respective functions;
- Implementing the delegated action plans to address the identified risks;
- Informing the management of new risks and significant changes in known risks; and
- Co-operating with other role players in the risk management processed and providing information as required.

SECTION 7. COMPONENTS OF ENTERPRISE RISK MANAGEMENT

The Group's Enterprise Risk Management framework is made up of six process components derived from the Committee of Sponsoring Organization of the Treadway Commission (COSO) ERM Framework. Objectives are set by the Board and the Executive Management and are cascaded throughout the organization.

1) Event Identification

As part of the strategic planning processes (strategic risk) and day-to-day management (operational risks) of the business, functional managers identify internal and external events that may affect the achievement of The Groups' objectives. It should be inclusive, not overly rely on the inputs of a few senior officers of the organization and should also draw as much as possible on unbiased independent sources, including the perspective of important stakeholders.

2) Risk Assessment

A systematic process used to quantify or qualify the level of risk associated with a specific threat or event, to determine how they should be managed. The main purpose is to help the organization to prioritize the most important risks as the organization is not expected to have the capacity to deal with all risks in an equal manner.

3) Risk Response

A response is determined based upon the overall risk exposure or opportunity, considered as a function of likelihood and impact of the occurrence. Risk or Opportunity responses may include avoiding or enhancing, accepting or ignoring, mitigating, exploiting, and sharing or transferring risk.

Responding to risks involves identifying and evaluating the range of possible options to mitigate risks and implementing the chosen option. The management should develop response strategies for all material risks.

4) Control Activities

Controls activities are established to ensure that risk or opportunity responses are carried out effectively and consistently throughout the organization. This involves formalizing risk response in our organization policies, ensuring clear accountability, utilizing self-assessment and monitoring tools and designing controls into our systems and critical business process.

Everyone in the organization should have responsibilities for maintaining effective systems of internal controls, consistent with their delegated authority. Internal controls include:

a. Preventive controls
b. Detective controls
c. Corrective controls
d. Management controls
e. Administrative controls
f. Accounting controls
g. Information technology controls

5) Information & Communication

Information and communication channels are in place to make the organization aware of risks that fall into their area of responsibility and expected behavior and actions to mitigate negative outcome.

The organization's risk communication and reporting process should support enhanced decision making and accountability through:

- Dissemination of relevant, timely, accurate and complete information; and
- Communication responsibilities and act.

6) Monitoring

The Management reviews, as well as assurance activities, such as testing, auditing and assessments, are in place to ensure that risks are effectively identified and assessed, and that appropriate responses, controls and preventive actions are in place. Monitoring should be effected through ongoing activities or separate evaluations to ascertain whether risk management is effectively practiced at all levels and across the organization in accordance with this Policy, strategy and plan.

Monitoring activities should focus on evaluating whether:

a. Allocated responsibilities are being executed effectively;
b. Response strategies are producing the desired result of mitigating risks or exploiting opportunities; and
c. A positive correlation exists between improvements in the system of risk management and organization performance.

While no risk management system can ever be absolutely complete, the goal is to make certain that identified risks are managed within acceptable levels.

SECTION 8. RISKS CATEGORIES

Risks to the Group's success will be grouped into four categories: (1) Strategic, (2) Operational, (3) Compliance and (4) Financial. Specific examples of each type of risk are included in the Table No. 1 in the following page.

Table No. 1: Risks Categories

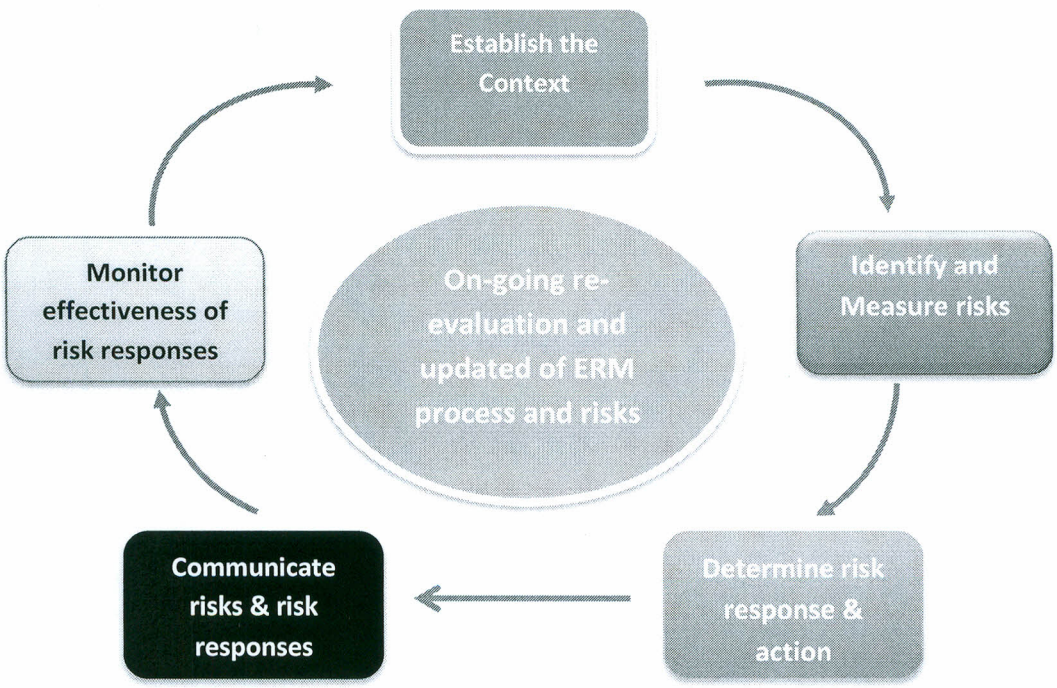
Risks Type	Definition & Examples
Strategic	Arise from the fundamental decisions that our Directors, Executive/Local Management take concerning an organization's product or services rendered. Essentially, strategic risks are risks that affect or are created by the Group's business strategy and strategic objectives. Examples: • Reduction in business vitality (due to change in business strategy, customer spending patterns, product discovery & changing technology, etc.) • Loss of intellectual property & trade secrets • Competition for talent • Negative impact to reputation/loss of public trust
Operational	Major risks that affect our organization's ability to execute the strategic plan. It resulted from inadequate or failed internal processes, people and systems or from external events. Examples: • Disruption of product supply • Counterfeiting • Inefficient use of resources/increased product or service cost • Physical property damage or disruption
Compliance	Risks of legal sanctions, material financial loss, or loss to reputation the Group may suffer as a result of its failure to comply with laws, our policies and code of business conduct, and best practices. Examples: Violations of laws or regulations governing areas such as: • Environmental • Employee health & safety • Clinical trial subject/patient safety • Product quality/safety issues • Selling and promotion of our products • Internal revenue or local tax, and legal laws
Financial	Risks associated with financing and financial transactions. • Credit/Default risks • Liquidity risks • Market risks • Financial misstatement

SECTION 9. THE ERM PROCESS

ERM is an on-going and cyclical process. The Board and Executive Management set the tone for enterprise risk management in The Group. This includes establishing The Group's risk tolerance, and how risks will be identified, measured and managed.

There are five primary steps in the ERM process, as indicated in the Illustration No. 1. It is also important to ensure that ERM process and risks are re-evaluated and updated on an on-going basis to reflect new information and experiences so that all significant risks are appropriately identified and addressed and that any material opportunities are not overlooked.

Illustration No. 1: ERM Cycle



Five Steps in the ERM process

These five steps will be performed by Local Management and Risk Owners in consultation with the Board, Audit Committee and Executive Management.

Step 1: Establish the Context

The purpose of establishing the context is to set the stage for risk identification. Since "risk" is defined as "any issue (positive or negative) that may impact an organization's ability to achieve its objectives," defining the organization's objectives is a prerequisite to identifying risk.

This involves understanding the Group or its department's objectives, and defining internal activities (e.g., hotel services, service repair, procurement, inventory, credit, billing, etc.) and external environment (e.g., laws, competition, social, economic, technological, reputation etc.) within which the Group operates.

Step 2: Identify and Measure Risks

The purpose of this step is to develop an understanding of the risk or opportunity in order to have informed evaluation and decision of whether a response is required. Generate a comprehensive list of threats and opportunities based on those events that might enhance, prevent, degrade, accelerate or delay the achievement of objectives; and identify its sources, causes and potential consequences. Comprehend the nature of the risk or opportunity and determine the level of risk exposure in terms of likelihood and impact using Tables 2 & 3 below as a guide.

Likelihood indicates the chance of a risk materializing in the given terms.

Table No. 2: Risk Likelihood

Score	Rating	Description
5	Almost Certain	> = 90 % chance of occurrence over life of asset, project or company.
4	Likely	= 65% to <90% chance of occurrence over life of asset, project or company.
3	Possible	= 35% to < 65% chance of occurrence over life of asset, project or company.
2	Unlikely	= 10% to < 35% chance of occurrence over life of asset, project or company.
1	Rare	< 10% chance of occurrence over life of asset, project or company.

Impact indicates the potential seriousness should the risk materialize.

Table No. 3: Risks Impact

Score	Rating	Description
5	Catastrophic	• Annual financial loss *(see table 4)* • Loss of reputation • Substantial prosecution and fines • Key business area closure
4	Major	• Annual financial loss *(see table 4)* • Significant effect on reputation • Significant prosecution and fines • Significant threat to key business area
3	Moderate	• Annual financial loss *(see table 4)*. • Adverse effect on reputation • Limited prosecution and fines • Limited threat to key business area
2	Minor	• Annual financial loss *(see table 4)*. • Minor adverse effect on reputation • No prosecution and fines • Minor threat to key business area
1	Negligible	• Annual financial loss *(see table 4)* • Minimal impact or no discernable impact at all.

Table 4: Annual Financial Loss Bracket

Revenue/Asset*	Catastrophic	Major	Moderate	Minor	Negligible
Above 1B	> 50M	>30M to 50M	>15M to 30M	>5M to 15M	5M or less
Above 500M to 1B	>30M	>20M to 30M	>10M to 20M	>5M to 10M	5M or less
Above 100M to 500M	>20M	>10M to 20M	>5M to 10M	>2M to 5M	2M or less
Above 50M to 100M	>10M	>5M to 10M	>2M to 5M	>1M to 2M	1M or less
50M and below	>5M	>3M to 5M	>1M to 3M	>0.5M to 1M	0.5M or less

* Use revenue or asset, whichever is lower as base in the assessment.

Step 3. Determine Risks Response and Action

The purpose of the risk response and action step is to decide, based on the results of measuring risks, which risks and opportunities require a response and what your recommended response will be.

a. **Opportunity response (treatment):** Process to modify or respond to an opportunity. Opportunity response can involve one or a combination of: enhancement, exploitation, ignoring, or sharing.

- **Enhance** – The opportunity equivalent of "mitigating" a risks is to enhance the opportunity. Enhancing seeks to increase the probability and/or the impact of the opportunity in order to maximize the benefit to the project or The Group.
- **Exploit** – Parallels the "avoid" response, where the general approach is to eliminate uncertainty. For opportunities, the "exploit" strategy seeks to make the opportunity definitely happen. Aggressive measures are taken which seek to ensure that the benefits from this opportunity are realized by the project or The Group.
- **Ignore** – just as the "accept" strategy takes no active measures to deal with a residual risk, opportunities can be ignored, adopting a reactive approach without taking explicit actions.
- **Sharing** – the "transfer" strategy for opportunities seeks a partner able to manage the opportunity who can maximize the chance of it happening and/or increase the potential benefits. This will involve sharing any upside in the same way as risks transfer involves passing penalties.

b. **Risk response (treatment)**. Process to modify or respond to a risk. Risks response can involve one or a combination of: accept, avoid, mitigate or transfer.

- **Accept –** If the risk impact is consistent with the Group's tolerance, the risk may be retained at the current level.
- **Avoid –** If the risk exposure far exceeds the Group's risk tolerance, the Group does not believe it can manage the risk, and the risk is not core to the Group's strategy, then the Group should consider avoiding.
- **Mitigate –** If the risk impact exceeds the Group's tolerance but management is confident that the risk can be reduce to a lower, more acceptable level, risk reduction is an appropriate management strategy.
- **Transfer –** If the risk impact is high relative to risk tolerance or the Group cannot believe it can manage the risk on its own but the risk is close to its cored or cannot be avoided, then the Group should consider sharing or transferring the risk to the third parties (e.g., insurance) who have the ability or capacity to accept or manage the risk.

Generally, if the magnitude or severity of the risk under consideration is high, the risk response needs to be strong (mitigate, transfer or avoid). Each risk and related response should be assigned to the manager who is responsible for the area affected by the risk. As part of the response process, management should determine and document what controls are necessary to manage the risk.

Step 4. Communicate risk and response

The Local Management submits the result of the risks analysis to the Executive Management and the Board at least annually (together with their Annual/Corporate Budget) or on a Project basis.

The report should contain at minimum as follows:

- Summary of materials risks and its risk scoring;
- Highlight of all material risks, and those risks that exceed the risk tolerance;
- Timeframe and status of risk management activities or risk responses for each risks;
- Risks that are getting worse, success of treatment plans, and risks that require additional attention;
- Highlights of any new risks including their risks assessment, risk response and management activities;
- Highlights of untreated risks and risk treatments that are overdue, and their risk owners;
- Material emerging risks; and
- Summary of exceptions to established policies or limits for key risks.

The Executive Management and the Board will conduct an annual review of all high risks areas (including those risks appropriately responded within risk tolerance) in order to have a full understanding of all the material risks facing the Group.

Step 5. Monitor effectiveness of risk responses

Risks and risk response activities will be monitored by the responsible Risk Owners and Local Management to ensure that significant risk remain within acceptable risk levels, that emerging risks are identified, and that risk response and control activities are effective and appropriate. Group Internal Audit and the Audit Committee role is to give reasonable assurance that management is monitoring and managing risks in accordance with established levels and this Policy.

The Audit Committee shall conduct regular assessment of risk management processes to identify opportunities for improvement; risk management standards used in other organization to ensure our Policy reflect contemporary best practices; and performance measures with regards to risk management in company strategies and performance's operational plan.

SECTION 10. RISK MANAGEMENT REQUIREMENTS

8.1 The Local Management is accountable for managing risks and must maintain a risk register relating to material risk exposures of their Company;

8.2 Risk registers should be based on the outcomes of thorough risk identification and assessment processes and in accordance with this Policy;

8.3 Review of risk registers are to be conducted at least annually or depends on business requirements, and reporting and escalations should occur in accordance with this Policy;

8.4 The Local Management should develop its own risk tolerance and submit to the Executive Management and the Board for approval.

8.5 Any changes to the risk rating/scoring due to business nature/complexity are subject to the Board's approval.

SECTION 11. ERM INTEGRATION

Risk management is part of the Group's strategy to promote accountability through good governance and robust business practices, which contributes to our strategic objective. In this regard, Local Management shall practice into its governance, planning, reporting, performance review, and improvement processes.

In order to integrate the ERM process in the Group business activities, the Executive Management requires that all reports communicated to them by Local Management such as but not limited to the reports below, shall also contain summary results of ERM process in accordance with Section 9 of this Policy.

a. Annual Corporate/Budget Plan including Strategic/Business Plan
b. Quarterly Financial Statement Reviews
c. Project Plan / Proposal
d. Capital Expenditure/Asset Acquisition/Expansion Plan
e. Major Repair Plan
f. Tax and Legal Management
g. Contracts
h. Policies and procedures
i. Key Performance Indicator (KPI) Reviews

The Local Management is required to document their ERM process implementation into their business activities and internal control formulation/improvement, which the Executive Management, Audit Committee or Group Internal Audit may request / obtain to review the results and the process.

SECTION 12. EFFECTIVITY

This Policy shall take effect immediately.

Approved by:

SUSAN L. TAN	**JOSEPH LIM**	**ELENA S. LIM**
Chairman of the Board	Director	Director
DAVID S. LIM	**JASON S. LIM**	**VINCENT S. LIM**
Director	Director	Director
BEDA T. MANALAC	**QUINTIN CHUA**	**LUIS MARIA ZABALJAUREGUI**
Director	Independent Director	Independent Director