ENTERPRISE RISK MANAGEMENT POLICY – SBS PHILIPPINES CORPORATION

Version 1.0

DOCUMENT INFORMATION

Title	*Enterprise Risk Management Manual*
Author	*Esmeraldo Tepace / Emerson Paulino*
Version	1.0
Date of Revision	
Status	Approved
Filename	ERM Manual

HISTORY

Version	Date	Description of changes
1.0	May 6, 2021	Final version

Table of Contents

1 Introduction

1.1 Risk Management Policy statement

SBS Philippines Corporation is committed to integrating risk management practices into its business strategy and performance to drive consistent, effective and accountable management in achieving the Company's business objectives.

SBS recognizes that risk is dynamic and is inherent in all external and internal operating environments, and that managing risks is vital in *defining the organization's purpose, process and expected results, which are the foundations of its daily operations.*

Effective risk management framework provides the means to ensure that all risks – operational, financial, compliance and regulatory, strategic and external/novel are identified, assessed, monitored, mitigated and controlled.

To meet this commitment, risk management should be every employee's business. All employees are responsible and accountable for managing risks within their area of responsibility and that the Board and senior management is responsible of its oversight. For this purpose, SBS will employ the "three lines of defense" approach where employees and associates involved in operations, line supervisors and managers and the compliance and audit staff are involved in actively managing the risks of SBS. The board of directors, on the other hand, is responsible for the oversight of this effort.

Through the Framework and its supporting processes, the organization formally establishes and communicates its risk limits.

There is a potentially higher appetite where benefits created by potential innovation or improvisation outweigh the risks. Benefits may include improved service delivery, and/or increased efficiency and effectiveness of the company's operations.

The framework follows the model of the *2017 Enterprise Risk Management – Integrating with Strategy and Performance of COSO or Committee of the Sponsoring Organizations of the Treadway Commission.*

In summary, the enterprise risk management practice of SBS Philippines Corporation is a continuous cycle of interrelated processes:

1.2 Purpose

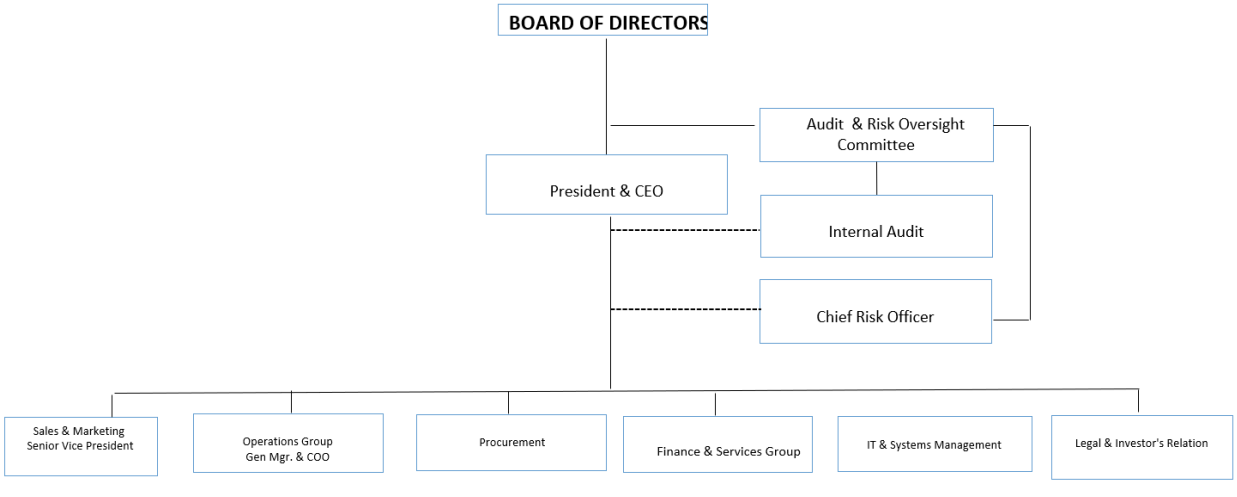
The Enterprise Risk Management Manual forms part of the Company's compliance policies and shall:

- Establish the risk management framework – the risk philosophy, strategy, objectives, policies and procedures of the Company;
- Define the roles and responsibilities of the Board, the senior management, and the entire work force;
- Communicate and provide rules or guidelines to the whole organization in the implementation of risk management practices;
- Provide baseline references for the internal and external audit activities as they perform their function in the risk evaluation, assessment and other related audit activities;
- Sets the scope and application of risk management within the organization; and
- Details the process of risk reporting obligations to external and internal stakeholders

1.3 Scope

The ERM Framework applies to SBS Philippines Corporation's functional departments and its processes and sub-processes. The diagram below represents the risk universe:

SBS ORGANIZATION CHART



1.4 Benefits

The enterprise risk management can realize many benefits, including, though not limited to:

• Increasing the range of opportunities: By considering all possibilities—both positive and negative aspects of risk—management can identify new opportunities and unique challenges associated with current opportunities.

• Identifying and managing risk entity-wide: Every entity faces myriad risks that can affect many parts of the organization. Sometimes a risk can originate in one part of the entity but impact a different part. Consequently, management identifies and manages these entity-wide risks to sustain and improve performance.

• Increasing positive outcomes and advantage while reducing negative surprises: Enterprise risk management allows entities to improve their ability to identify risks and establish appropriate responses, reducing surprises and related costs or losses, while profiting from advantageous developments.

• Reducing performance variability: For some, the challenge is less with surprises and losses and more with variability in performance. Performing ahead of schedule or beyond expectations may cause as much concern as performing short of scheduling and expectations. Enterprise risk management allows organizations to anticipate the risks that would affect performance and enable them to put in place the actions needed to minimize disruption and maximize opportunity.

• Improving resource deployment: Every risk could be considered a request for resources. Obtaining robust information on risk allows management, in the face of finite resources, to assess overall resource needs, prioritize resource deployment and enhance resource allocation.

• Enhancing enterprise resilience: An entity's medium- and long-term viability depends on its ability to anticipate and respond to change, not only to survive but also to evolve and thrive. This is, in part, enabled by effective enterprise risk management. It becomes increasingly important as the pace of change accelerates and business complexity increases.

These benefits highlight the fact that risk should not be viewed solely as a potential constraint or challenge to setting and carrying out a strategy. Rather, the change that underlies risk and the organizational responses to risk give rise to strategic opportunities and key differentiating capabilities.

1.5 Critical Success Factors

Enjoying the benefits of the success of risk management depends upon:

- The board and senior management setting the tone for the whole organization towards risk management being an integral part of strategic, project and operational planning and activities throughout all levels of the Group;
- Risk management being openly accepted and supported by the organization's leadership as providing good business value, with this acceptance reinforced through avenues such as managers and staff performance requirements and making it part of their performance assessment criteria;
- trained and mindful employees who are capable of understanding the impact of risk on their work and utilize risk management practices while performing their tasks;
- Effective evaluation and monitoring from appropriate functions – internal audit, external audit, compliance and controls team; and
- Appropriate pre-emptive and post-risk event responses by management.

2 Enterprise Risk Management

2.1 Definition of terms

Enterprise Risk Management as defined by COSO as follows:

> *Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.*

The definition reflects certain fundamental concepts. Enterprise risk management is:

• A process, ongoing and flowing through an entity

• Effected by people at every level of an organization

• Applied in strategy setting

• Applied across the enterprise, at every level and unit, and includes taking an entity level *portfolio* view of risk

• Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite

• Able to provide reasonable assurance to an entity's management and board of directors

• Geared to achievement of objectives in one or more separate but overlapping categories

Other terms:

Audit & Risk Oversight Committee of the Board - is the board committee designated to oversee the enterprise risk management program of the company.

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

A few misconceptions about enterprise risk management should be clarified as follows:

Enterprise risk management is not a function or department. It is the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing value.

Enterprise risk management is more than a risk listing. It requires more than taking an inventory of all the risks within the organization. It is broader and includes practices that management puts in place to actively manage risk.

Enterprise risk management addresses more than internal control. It also addresses other topics such as strategy-setting, governance, communicating with stakeholders, and measuring performance. Its principles apply at all levels of the organization and across all functions.

Enterprise risk management is not a checklist. It is a set of principles on which processes can be built or integrated for a particular organization, and it is a system of monitoring, learning, and improving performance.

2.2 Framework Model

As stated in 1.1 Risk Management Policy Statement, this framework follows the model of 2017 COSO framework:

Enterprise Risk Management—Integrating with Strategy and Performance is a framework tha focuses on the importance of enterprise risk management in strategic planning and embedding it throughout an organization—because risk influences and aligns strategy and performance across all departments and functions.

2.3 Components

The Framework itself is a set of principles organized into five interrelated components:

1. Governance and Culture: Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviours, and understanding of risk in the entity.

2. Strategy and Objective-Setting: Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.

3. Performance: Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.

4. Review and Revision: By reviewing its performance, the Company can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.

5. Information, Communication, and Reporting: Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.

These principles are the guiding components of this framework and are discussed in detail in the subsequent sections of this manual.

3 Governance & Culture

3.1 Oversight Structure

The Board of Directors and senior management are responsible for overseeing the enterprise-wide risk management practices, which are integrated within the three lines of defense in the Company's operations:

The ***first line of defense*** rests with the process owners, analysts, line supervisors and managers of the Operations, Operations – Support and the Shared Services team, who primarily executes, initiates and performs the policies and procedures of the Organization. They are responsible for ensuring that risks are assessed and acted upon in their daily functions - which includes but not limited to customer evaluation and profiling, record keeping, reporting and human resource recruitment, - in accordance with this Framework Manual.

The ***second line of defense*** lies with the Risk Management and Compliance functions. Risk Management are responsible for the management of the company's risk management activities; and to check for any risk issues that the first line of defense might not have prevented or detected. Compliance functions are responsible to ensure that the company complies with applicable government rules and regulations. This includes, but not limited to: Regulatory, Health & Safety and Quality Control.

The ***third line of defense*** is the Audit functions which includes both Internal and External (i.e. 3rd party Financial Auditors). Internal Audit provides an independent, objective assurance on risk management, controls and corporate governance processes, while External Audit provides an independent and reasonable assurance on the company's financial statements.

3.2 Roles & Responsibilities

Below are the roles and responsibilities of key stakeholders in regards to the Risk Management Framework:

Key Stakeholder	Roles & Responsibilities
Audit and Risk Oversight Committee of the Board	In the exercise of its oversight role, may include, but not be limited to the following: • Review annually the organization's risk profile; • Provide oversight on significant risk exposures and control issues, including fraud risk, governance issues, and other matters needed or requested by senior management and the board; • Obtain from Internal Audit an annual report on management's implementation and maintenance of an appropriate enterprise risk management processes; • Review and provide advice on the risk management processes established and maintained by management and the procedures in place to ensure that they are operating as intended; • Ask management to propose to and advise the Board on the appropriate risk appetite levels and risk tolerance limits for the Company. • Monitor and review, together with the Company's internal audit division, the adequacy and effectiveness of the Company's internal controls, the security of physical and information assets and Management's response to Internal Audit findings and recommendations;
Senior and Executive Management	• Risk management planning and implementation under the leadership of the President; • Propose to the Board the appropriate risk appetite levels and risk tolerance limits for the Company • 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 will be business/project-specific; and • Establishing a sound risk aware culture throughout the enterprise.
Internal Audit	Provides assurance on the following: • Risk management processes are performing as intended; • Controls and key responses on key risks are effective and complied; and • Established policies and procedures are being complied with. • Provides assessment of the ERM framework
Risk Management	• Update the ERM Manual as necessary • Prepare, coordinate, and update the Risk Register with the business units to identify and monitor risk responses (i.e. action plans / controls)
Regulatory Compliance	• Manage and coordinate compliance with regulatory authorities • Facilitate processing of required permits and licenses • Prepare and coordinate the Risk Register with the business units to identify and monitor risk responses (i.e. action plans / controls)
Staff / Supervisors / Managers	• Maintain awareness on the intrinsic risks in their jobs and its management as part of their performance management. • Incorporate risk management as part of their everyday activities. • Take charge of their respective internal control as part of their accountability in achieving their objectives.

4 Strategy & Objective Setting

4.1 Mission, Vision and Core Values

VISION

Our personal aspiration and business endeavor is,

"To be the best-in-class chemical raw materials provider and the chemical supplier of choice"

MISSION

Our mission is to create a legacy of growth by creating value for all stakeholders:

- By bringing in returns for our investors and shareholders
- By meeting the sourcing requirements of our customers
- By improving market penetration for our suppliers
- By ensuring the safety and well-being of our employees
- By contributing to resource efficiency and environmental sustainability for the community

OUR GOAL

We strive to achieve this goal by:

- Distributing a wide-range of top quality and cost-efficient products
- Extending reliable customer service at all times
- Nurturing strong, long-term relationships with suppliers and customers
- Constantly seeking new markets and new opportunities
- Continously improving our internal business processes and systems

CORE VALUES

- Honesty and Integrity
- Hard work and Perseverance
- Productivity and Excellence
- Customer Satisfaction
- Loyalty and Dedication
- Faith in God Almighty

4.2 The Role of Risk in Strategy Selection

Enterprise risk management is integrated into the business strategy, as this is the best approach for the management to make well-informed choices.

As this Framework emphasizes, there are two additional aspects to enterprise risk management that can have far greater effect on an entity's value: the possibility of the strategy not aligning, and the implications from the strategy chosen.

1. **The possibility of the strategy not aligning** - A chosen strategy must support the organization's mission and vision. A misaligned strategy increases the possibility that the organization may not realize its mission and vision, or may compromise its values, even if a strategy is successfully carried out. Therefore, enterprise risk management considers the possibility of strategy not aligning with the mission and vision of the organization.
2. **Implications from the strategy chosen -** Each alternative strategy has its own risk profile—these are the implications arising from the strategy. The board of directors and management need to determine if the strategy works in tandem with the organization's risk appetite, and how it will help drive the organization to set objectives and ultimately allocate resources efficiently.

Enterprise risk management is as much about understanding the implications from the strategy and the possibility of strategy not aligning as it is about managing risks to set objectives. The figure below illustrates these considerations in the context of mission, vision, core values, and as a driver of an entity's overall direction and performance:

4.3 Objective Setting

This framework establishes four categories of entity objectives that the Company aims to achieve:

• **Strategic** – are high-level goals, aligned with and supporting the entity's mission/vision. This reflect management's choice as to how the entity will seek to create value for its stakeholders.

Related Objectives:

• **Operational** – These pertain to the effectiveness and efficiency of the entity's operations, including performance and profitability goals and safeguarding resources against loss. They vary based on management's choices about structure and performance.

• **Financial Reporting** – relating to the reliability of the entity's reporting (i.e. financial statements)

• **Compliance** – relating to the entity's compliance with applicable laws and regulations

The Company's mission sets out in broad terms what the entity aspires to achieve. Whatever term is used, such as "mission," "vision," or "purpose," it is important that management – with board oversight – explicitly establish the entity's broad-based reason for being. From this, management sets strategic objectives, formulates strategy, and establishes related operations, compliance, and reporting objectives for the organization.

By focusing first on strategic objectives and strategy, an entity is positioned to develop related objectives at an entity level, achievement of which will create and preserve value. Entity-level objectives are linked to and integrated with more specific objectives that cascade through the organization to sub-objectives established for various activities, such as sales, production, and engineering, and infrastructure functions.

5 Risk Management Performance

After identifying the business objectives or basically, what the Company wants to accomplish, risks can now be determined. Risk is defined as the possibility that an event will occur and affect – either positively or negatively - the achievement of objectives.

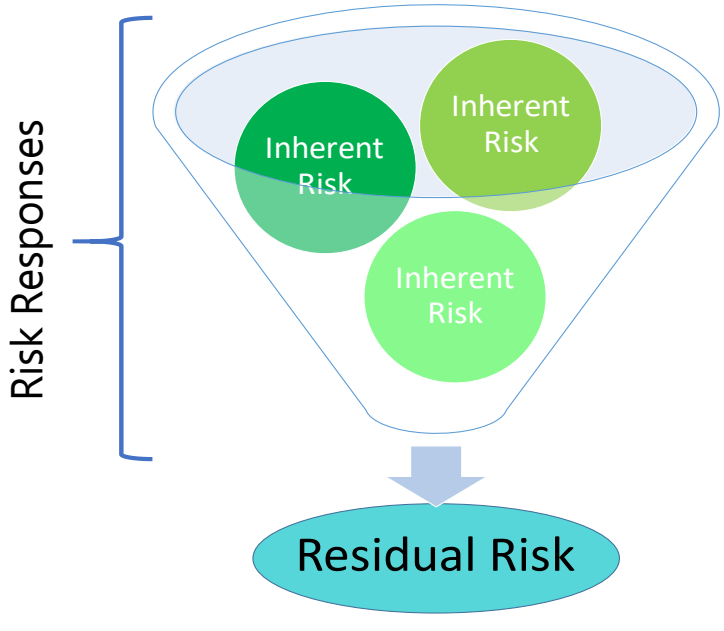
The Risk Process flow consists of - Risk Identification, Risk Assessment, Risk Prioritization and Responding to Risks:

5.1 Risk Identification

Risks are identified for each objective set by the management. Risks are generally classified as Inherent or Residual:

- Inherent Risk - is the risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact.
- Residual Risk - is the risk that remains after management's response to the risk

Risk assessment is applied first to inherent risks. Once risk responses have been developed, management then considers residual risk. The figure below illustrate this process:



The identified risks are compiled in the risk register of the company which serves as the repository for all risks identified and includes additional information about each risk, e.g. objective, nature of the risk, reference and owner, evaluation, risk responses etc.

5.2 Risk Assessment

Assessing risks consists of assigning values to each risk using defined criteria. This is accomplished in two stages where an initial screening of the risks is performed using qualitative techniques followed by a more quantitative analysis of the most important risks.

As already defined, Risk is defined as the possibility that an event will occur and affect – either positively or negatively - the achievement of objectives which is evaluated from two perspectives or criteria – likelihood and impact.

Impact

Impact (or consequence) refers to the extent to which a risk event might affect the enterprise. Impact assessment criteria may include financial, reputational, regulatory, health, safety, security, environmental, employee, customer, and operational impacts. Enterprises typically define impact using a combination of these types of impact considerations (as illustrated below), given that certain risks may impact the enterprise financially while other risks may have a greater impact to reputation or health and safety. Sample Risk Scale for Impact below:

Rating	Description	Financial	Operational	Legal & Compliance	Human Resource	Environment Health & Safey	Image & Reputation
1	**Low**	- Financial loss is less than 5% of Net Income or Equity from previous calendar year	- Delay or disruption in operations is from zero to 1 man day	- Minor legal issues - Not reportable to regulator(s)	- Isolated employee dissatisfaction	- No injuries to employees or third parties	- Local media attention quickly remedied
2	**Average**	- Financial loss is more than 5% but less than 10% of Net Income or Equity from previous calendar year	- Delay or disruption in operations is 2 to 6 man days	- Potential litigation with minor penalties - Potential reportable issues to regulator(s) but management action plan in place	- Staff morale problems increases turnover	- Minor injuries to employees or third parties	- Local media attention causes some concern for stakeholders
3	**High**	- Financial loss is more than 10% but less than 15% of Net Income or Equity from previous calendar year	- Delay or disruption in operations is from 7 to 14 man days	- Significant litigation with punitive fines - Reportable issues to regulator(s) but management action plan in place	- Widespread staff morale problems and high turnover	- Out-patient medical treatment required for injuries	- National short-term negative media coverage
4	**Extreme**	- Financial loss is more than 15% of Net Income or Equity from previous calendar year	- Delay or disruption in operations is indefinite	- Major litigation with major costs and may lead to company closure - Reportable incident requiring major change management or business shutdown	- Senior managers leave, high turnover of experienced staff	- Significant injuries which may require in-patient care to employees or third parties or which may lead to death	- National long-term negative media coverage

Likelihood

Likelihood represents the possibility that a given event will occur. Likelihood can be expressed using qualitative terms (frequent, likely, possible, unlikely, rare), as a percent probability, or as a frequency. When using numerical values, whether a percentage or frequency, the relevant time period should be specified such as annual frequency or the more relative probability over the life of the project or asset. Sometimes enterprises describe likelihood in more personal and qualitative terms such as "event expected to occur several times over the course of a career" or "event not expected to occur over the course of a career." Sample Risk Scale for Likelihood below:

Rating	Descriptor	Chance of Occurrence
1	**Unlikely**	- less than 10% chance of occurrence or probability - No known occurrence yet or last occurrence more than 25 years ago
2	**Possible**	- 10% to 35% chance of occurrence or probability - Last occurrence was more than 15 years
3	**Probable**	- 36% to 65% chance of occurrence or probability - Last occurrence was 10 years ago
4	**Likely**	- 66% to 90% chance of occurrence or probability - Last occurrence was 5 years ago
5	**Almost Certain**	- More than 90% chance of occurrence or probability - Last occurrence was 2 years ago

Each risk identified is assessed by management and assigned a rating scale for both likelihood and impact. There are assessment techniques that can be used so that management can reasonably evaluate and assign ratings to the risks identified.

5.3 Risk Prioritization

Risk prioritization is the process of determining risk management priorities by comparing the level of risk against predetermined target risk levels and tolerance thresholds. This is done by determining the risk level by combining both criteria - impact and likelihood so that management can evaluate what risk(s) should be acted upon first and what actions or non-actions should be taken.

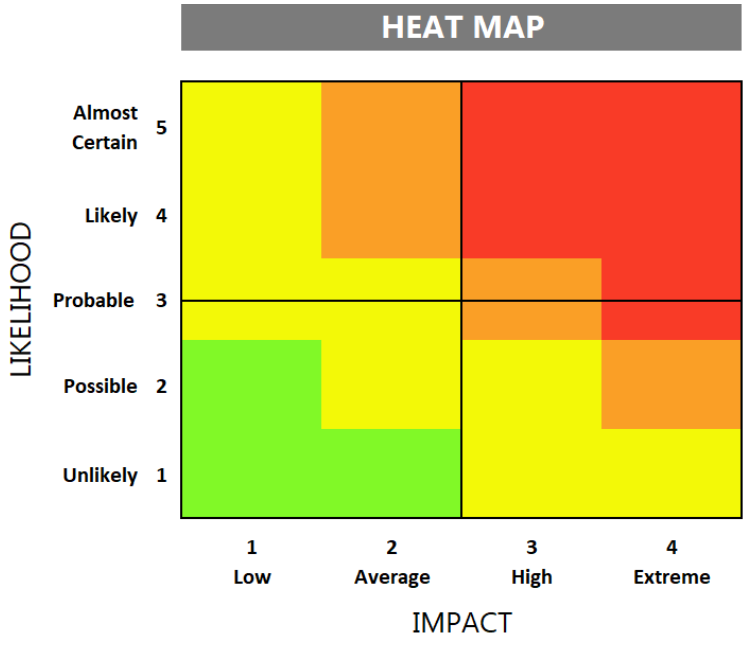
Risk Maps

The most common and simple way to view the portfolio is to create a risk map, often called a heat map. These are usually two-dimensional representations of impact plotted against likelihood. They can also depict other relationships such as impact versus vulnerability. For even richer information, the size of the data points can reflect a third variable such as speed of onset or the degree of uncertainty in the estimates.

The most common way to prioritize risks is by designating a risk level for each area of the graph such as very high, high, medium, or low, where the higher the combined impact and likelihood ratings, the higher the overall risk level. The boundaries between levels vary from entity to entity depending on risk appetite. For example, an entity with a greater risk appetite will have boundaries between risk levels shifted toward the upper right, and an entity with greater risk aversion will have boundaries between risk levels shifted toward the bottom left.

After plotting on the heat map, risks are then ranked from highest to lowest in terms of risk level. These rankings may then be adjusted based on other considerations such as vulnerability, speed of onset, or detailed knowledge of the nature of the impact. For example, within a group of risks having a designation of very high, those risks having extreme health and safety or reputational impacts may be prioritized over risks having extreme financial impacts but lesser health and safety or reputational impacts.

When using numerical ratings in a qualitative environment, it's important to remember that the numbers are labels and not suitable for mathematical manipulation although some entities do multiply the ratings, such as for impact and likelihood, to develop a preliminary ranking.



From this heat map, management plots the risk rating – impact and likelihood for each identified risk. The heat map has colors that may represent the level of risks – green area pertains to the lowest level and the red area means the highest level. We can also assess that moving from bottom left to the upper right of the map translates to risk level increasing from lowest to highest.

5.4 Risk Response

Risk response (treatment) is a 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 company's tolerance, the risk may be retained at the current level.

• **Avoid** - If the risk exposure far exceeds the company's risk tolerance, the company does not believe it can manage the risk, and the risk is not core to the company's strategy, then the company should consider avoiding.

• **Mitigate** - If the risk impact exceeds the company'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 company cannot believe it can manage the risk on its own but the risk is close to its cored or cannot be avoided, then the company 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.

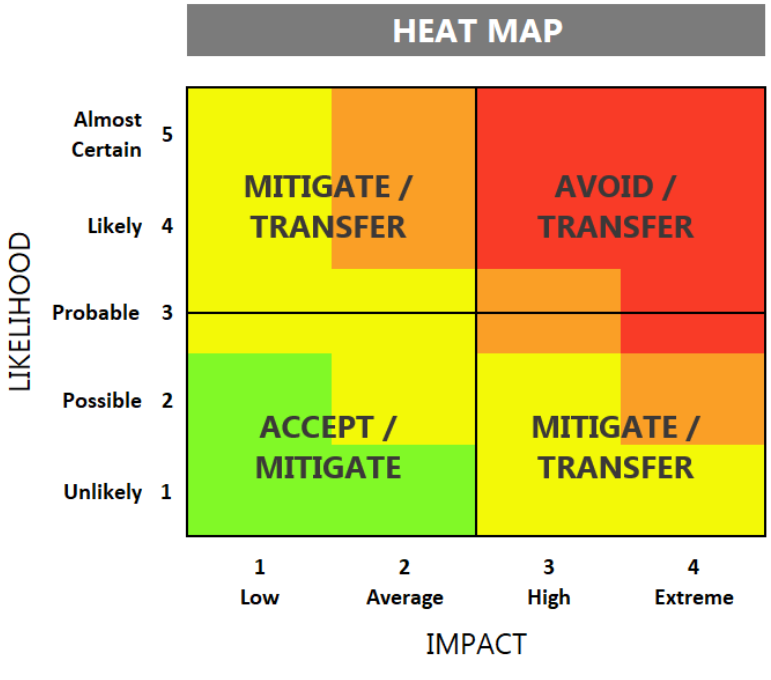
In determining risk response, management should consider such things as:

• Effects of potential responses on risk likelihood and impact – and which response options align with the entity's risk appetite or tolerance

• Costs versus benefits of potential responses

• Possible opportunities to achieve entity objectives going beyond dealing with the specific risk

Management can assign default risk responses on the risk levels in the heat map as shown below:



To further explain, risks falling on the *Accept / Mitigate* cube of the heat map may be treated with acceptance of risks by the management or that they may choose to establish a control to prevent or detect these risks. In regards to the risks falling on the highest level – *Avoid / Transfer*, the management should either transfer the function or deparment responsible for the risk or totally avoid the risks by ceasing to operate a function or department that contains the risk(s).

Evaluating Effect on Risk Likelihood and Impact

In evaluating response options, management considers the effect on both risk likelihood and impact, recognizing that a response might affect likelihood and impact differently.

In analyzing responses, management may consider past events and trends, and potential future scenarios. In evaluating alternative responses, management typically determines their potential effect using the same, or congruent, units of measure as those used for the related objective.

Assessing Costs versus Benefits

Cost/benefit analysis the process of weighing the expected costs against the expected benefit of one or more actions in order to choose the most appropriate option. Example, it may consider investing in a sales recording system or even an ERP system if the benefits include easier and real time reporting of customer transactions and detection of any red flags or potential violation(s).

However, management should be aware that cost and benefit measurements for implementing risk responses are made with varying levels of precision. Generally, it is easier to deal with the cost side of the equation, which, in many cases, can be quantified fairly precisely. All direct costs associated with instituting a response, and indirect costs where practically measurable,
usually are considered.

Opportunities in Response Options

Events with positive impacts represent opportunities and are channeled back to the strategy or objective setting processes. Similarly, opportunities may be identified when considering risk response. Risk response considerations should not be limited solely to reducing identified risks, but also should include consideration of new opportunities for the entity. Management may identify innovative responses, which, while fitting within the response categories may be entirely new to the entity or even an industry. Management's primary objective in sending its key officers to a risk, governance and controls workshop, for example, is to comply to an action plan from a recently performed audit. But in addition, the key officers can gain tools and techniques which enables them to design and implement effective and efficient control environment in the organization.

Selected Responses

Once the effects of alternative risk responses have been evaluated, management decides how it intends to manage the risk, selecting a response or combination of responses designed to bring risk likelihood and impact within risk tolerances. The response need not necessarily result in the least amount of residual risk. But where a risk response would result in residual risk exceeding risk tolerance, management revisits and revises the response accordingly or, in certain instances, reconsiders the established risk tolerance. Accordingly, the balancing of risk and risk tolerance may involve an iterative process.

Management recognizes that some level of residual risk will always exist, not only because resources are limited, but also because of future uncertainty and limitations inherent in all activities.

After identifying the "initial" risk responses for each risk, management can then evaluate how much residual risks (per impact and likelihood) will remain. Again, quantitative and qualitative evaluation can be used. If the residual risks is within the management's risk appetite, they may settle with the risk response. Otherwise, management can choose to identify other risk responses which may bring down the residual risk ratings to their risk appetite.

5.5 Risk Register

Risk Register is a document which contains the portfolio of risks of the company. It is a working tool for the management in managing risks. Risk registers does not have standard formats but, at the minimum, must reflect and contain the results of the risk management process – identification, assessment, prioritization and responses.

The risk register should be the primary document of reference when reviewing and monitoring the Company's actual risk management practices.

Objective Setting			Identify Risks		Risks - Inherent		Risk Response		Risks - Residual	
Objective Category	Risk Area	Objective	Risk ID	Risk Description	Impact	Likelihood	Response	Description	Impact2	Likelihood2
Operational	Operations	Establish customer service protocols and ensure that it is being observed	OP - 001	Customers do not receive quality service leading to dissatisfaction or lost sales	2	1	Accept	No additional control will be implemented as this risk can be mitigated by other controls such as training of operation personnel and supervision of Operation Supervisors.	2	1
Operational	Operations	Provide channels to identify customer needs and concerns	OP - 002	Customer needs and concerns are not addressed leading to lost opportunity or sales	2	4	Reduce	Customer survey form which will be part or a marketing program that aims to encourage customers to answer to gather information on their concerns and needs for service improvement.	2	2
Operational	Human Resources	Ensure that Customer Service courses are provided to new hires and refresher trainings	HR - 001	Operations are not aware of the Company's standards on customer service leading to customer dissatisfaction or lost sales	1	3	Reduce	New employees undergo a new hire orientation while existing employees undergo a refresher training on the Company's standards on customer service.	1	2
Financial	Accounting	Ensure that proper accounting policy and procedures are implemented in the system being used in the branches for proper recording of branch sales and expenses	AC - 001	Branch sales and expenses are not properly recorded leading to incorrect sales and expenses reporting.	3	2	Share	Accounting of branch operations, including sales and expenses is outsourced to third party service provider.	1	1
Compliance	Compliance	Ensure that warehouses only maintain inventories which are included in the business registration and applicable licenses and permits.	CA - 001	Warehouses maintain inventories which are NOT included in the business registration and applicable licenses and permits.	3	1	Reduce	A periodic compliance check will be performed by the Compliance Team on the branch operations.	2	1

6 ERM Integration

Risk management is part of the company'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 company 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.

7 Review and Revision

7.1 Continuous Improvement

Some of the processes that support continuous improvement and review of the Enterprise Risk Management Framework include:

- Daily practice and assessment of the risk management processes by the first and second line of defense – operational staffs and associates and their line supervisors and managers
- Regular audits and process reviews of both the Audit and Compliance functions, respectively
- Regular review and evaluation (i.e. *Institutional Risk Assessment*) of the Risk Register by the management and the Board
- Training and continuous development activities of the management pertaining to risk management
- Update of the COSO framework that may move the Board to adapt some or all of its provisions and guidelines

7.2 Frequency of update

This manual is reviewed every year by the Chief Risk Officer and Senior Management. Any change(s) is approved by the Board, through the Audit and Risk Oversight Committee.

7.3 Accountability

The Board, in its oversight role, should ensure that ERM Framework is reviewed and updated, as necessary, in accordance to this manual. However, this accountability is delegated to the Chief Risk Officer as the primary function to update the ERM framework.

8 Information, Communication & Reporting

8.1 Risk Awareness Program

The Risk Management function shall develop a risk awareness program, in coordination with other departments, which includes the following:

- Facilitation of regular trainings on risk management
- Regular meetings with line supervisors and managers on their risk accountabilities and their action plans
- Posting of infographic or other similar ads on visible areas in the company premises relating to risk management, especially on the Health and Safety protocols
- Open door policy that will encourage *whistle blowers* to report any risk concerns and issues
- Risk Awareness briefings
- Incident reporting process (in coordination with the Human Resources policies & procedures) which may expose risk concerns and issues within the business units

8.2 Nature & Timing of Reports

The following are the standard or baseline risk reports to be prepared, reviewed and approved:

Reports	Description / Purpose	Department Responsible	Reporting to	Frequency
Review of Risk Register	Review the Pawnshop's entire risk portfolio and corresponding action plans with risk owners (includes Compliance risks)	Risk Management	Board of Directors	Annual
Internal Audit plan	Finalize the audit priorities for the year in accordance with the ERM and Board objectives	Internal Audit	Board of Directors	Annual
Internal Audit reports	Report the audit results with management action plans	Internal Audit	Board of Directors	As per audit plan