Enterprise Risk Management Program Manual

Table of Contents

I. INTRODUCTION

The Enterprise Risk Management (ERM) Program

Establishing the ERM Program

The Board of Directors ("Board") and the Management of Citicore Energy REIT Corp. ("CREIT" or the "Company") fully recognizes the strategic value of an Enterprise Risk Management (ERM) system in running its day-to-day operations. It serves as a framework for an effective and sustainable management of uncertainties, mitigating prioritized risks, and exploring opportunities as they arise. It provides the Board and Management with an integrated and comprehensive methodology, and proactive approaches to identify, evaluate, and mitigate prioritized risks, as well as manage inherent and residual enterprise risks within the Company's risk appetite limit.

For this reason, the Company has established an Enterprise Risk Management (ERM) Program in managing imminent and emerging risks in its internal and external operating environments. Under the ERM Program, the Company shall appropriately respond to risks and manage them in order to protect and create, among others, shareholder value.

The ERM Program is aligned with the Company's Manual of Corporate Governance which mandates the Board of Directors to ensure the presence of organizational and procedural controls supported by an effective risk management system.

In addition, the Charter of the Company's Audit and Risk Oversight Committee mandates it to provide oversight to management functions relating to strategic, financial, operational, and other risks of the Company which involves periodic disclosure of risk exposures and related risk management activities.

The ERM Program aims to enhance shareholder value and improve competitive advantage by effectively managing risks through a standard and informed decision-making mechanism under a common risk culture and language understood by every individual within the Company.

The Company shall be highly valued for its ERM Program. The ERM Program shall be a globally-competitive tool, embedded into the Company's culture, adhering to the principles of good and effective corporate governance in the pursuit of powering a first- world Philippines.

Adoption of the Enterprise Risk Management (ERM) Program Manual

In order to fully and effectively implement and ensure compliance with the Enterprise Risk Management (ERM) Program, the Board hereby adopts this Enterprise Risk Management (ERM) Program Manual (Manual).

This Manual shall provide guidance on the implementation of the Company's ERM Program. This document describes basic concepts and explains the risk management process employed by the Company which shall be used by risk practitioners in the Company. This Manual shall provide managers a comprehensive and uniform approach to risk management.

Definition of Terms

Whenever and wherever used in this Manual, the following terms shall mean:

Audit and Risk Oversight Committee – the committee which assists the Board in fulfilling its responsibility for oversight of the Company's risk management activities.

Brainstorming - a group activity which involves stimulating and encouraging free-flowing conversation to gather ideas from group members about a particular issue.

Business Risk Dictionary – a tool that sets the common risk language within an organization.

Checklists – a tool that contains any list (e.g. list of risk or controls) that have been developed from past experience or historical data.

Chief Risk Officer – the champion of ERM at an organization; leads the development, implementation, maintenance and continuous improvement of a comprehensive Enterprise Risk Management (ERM) Program.

Context – the external and internal parameters to be considered when managing risk.

Control – a measure, strategy, program, activity or any mechanism in place that modifies the risk.

Communication and Consultation – a continual and iterative process that an organization conducts to provide, share or obtain information, and to engage in dialogue with stakeholders and others regarding the management of risk.

Document Review – a technique of going over documents to look for information that is relevant and useful.

Enterprise Risk Management - 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 risks to be within its risk appetite, and to provide reasonable assurance regarding the achievement of entity objectives.

Impact - measure of the tangible and intangible effects (consequences) of a risk in an enterprise.

Interview - a technique of obtaining information by one person (interviewer) from another (interviewee). The interviewer asks the interviewee questions about a specific topic, and the latter gives answers based on knowledge or expertise.

Key Risk Indicator – a measure of risk exposure and serves as the warning sign that the risk might possibly happen.

Likelihood – measure of the probability of a risk occurrence.

Monitoring – continual checking, supervising, critically observing, or determining the status in order to identify change from the performance level required or expected.

Questionnaire – a data collection technique in which people are asked to answer a set of predetermined questions. It may be self-administered or interview- administered, paper-based or electronic.

Residual Risk – risk remaining after risk treatment.

Review – activity undertaken to determine the suitability, adequacy, and effectiveness of the subject matter to achieve desired or established objectives.

Risk – the effect of uncertainty on objectives.

Risk Analysis – the process to comprehend the nature of risk and to determine the level of risk.

Risk Appetite - amount and type of risk that an organization is prepared to pursue, take or retain.

Risk Assessment – the overall process of risk identification, risk analysis, and risk evaluation.

Risk Assessment Criteria – terms of reference against which the significance of risk is evaluated.

Risk Driver Analysis – a tool to present and understand the underlying drivers and causes of risks. This is similar to the more common Root Cause Analysis, where risk drivers and sources are determined.

Risk Evaluation – the process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or magnitude is acceptable or tolerable.

Risk Identification – the process of finding, recognizing and describing risks.

Risk Management - coordinated activities to direct and control an organization with regard to risks.

Risk Management Executive Committee – a management committee responsible for defining risk priorities, aligning risk policies and strategies with overall company plan.

Risk Management Framework - set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing, and continually improving risk management throughout the organization.

Risk Management Policy - statement of the overall intentions and direction of an organization related to risk management.

Risk Management Process - systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring, and reviewing risks.

Risk Profile Map - a graphical depiction of a select number of a company's risks designed to illustrate the impact or significance of risks on one axis and likelihood on the other. Risk profile maps are used to assist in identifying, prioritizing, and quantifying (at a macro level) risks to an organization. This representation often takes the form of a two- dimensional grid with impact on one axis, and likelihood on the other axis; the risks that fall in the high impact/high likelihood quadrant are given priority risk-management attention.

Risk Matrix - a tool used in risk assessment that determines the level or rating of the risks by defining ranges for certain criteria.

Risk Owners – individuals that have the overall accountability for and ownership of the assigned risks and other risks in his functional areas of responsibility; manage risks at source.

Risk Profile – description of any set of risks.

Risk Register – a tool for documenting risks, and actions to manage each risk.

Risk Treatment – the process to modify the risks.

Scenario Analysis - a process that identifies possible future events by considering possible alternative outcomes. Consequently, it is used to identify risks assuming each of these alternative future events might occur. This can be done formally or informally and qualitatively or quantitatively.

Stakeholder - person who or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

II.   THE ERM FRAMEWORK
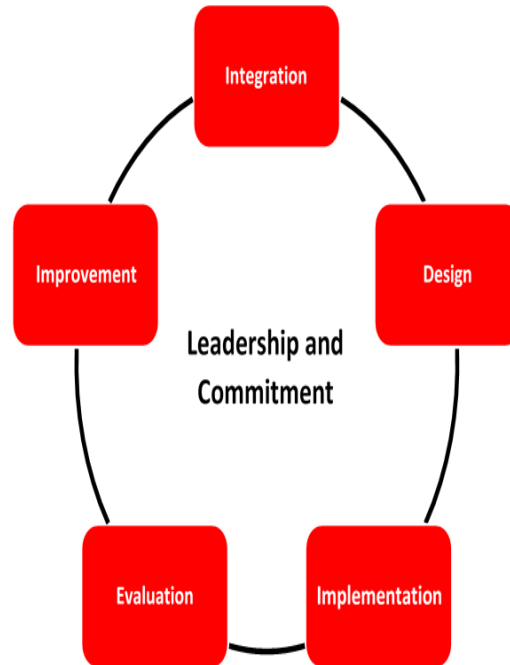
The ERM Framework

The CREIT ERM Framework is customized to the Company's and individual business units' operating environment and aligned on the recently published ISO 31000:2018 which contains standards relating to risk management codified by the International Organization for Standardization. The purpose of ISO 31000:2018 is to provide principles and generic guidelines on risk management. It seeks to provide a universally-recognized standard for practitioners and companies employing risk management processes to replace the myriad of existing principles, standards, and methodologies that differed between and among industries.

As part of its legal and regulatory compliance requirements, the Company implements this ERM Framework. To ensure its effective and sustainable implementation, the Company ensures the alignment of the following components: the ERM process and Company culture; ERM objectives and Company objectives; and key risk indicators (KRIs) and key performance indicators (KPIs). Specific accountabilities and responsibilities shall be established and necessary resources shall be allocated to set the process into motion.

Leadership and Commitment

The Framework is anchored on the leadership and commitment of the Board of Directors and top Management to implement the ERM Program across the Company. It is envisioned to be dynamic and shall be continuously improved in order to be responsive to the needs of the Company and attain their desired state.

Integrating Risk Management

Everyone is a Risk Manager. This vision can only be achieved once the risk management mindset has been integrated and embedded into the Company's organizational purpose, governance, leadership and commitment, strategy, objectives, and operations.

Integrating risk management in the Company is a dynamic and iterative process and was customized to address their needs and culture.

Design of Framework for Managing Risk

Designing the Company's ERM Framework required a thorough understanding of both the internal and external environments in which it operates. The external environment includes, but is not limited to, the cultural, technological, legal, financial and regulatory environment, its relationships with stakeholders, as well as industry and international trends. Its internal context includes company culture and values, policies and procedures, guidelines, organizational structure, and such other parameters that are internally driven.

The key components in the design of the ERM Framework are setting the common risk language and establishing the oversight structure.

Common Risk Language

The Company's Business Risk Dictionary, which is the basis for the development of a common risk language, shall be reviewed and updated to include emerging risks at least once a year during the annual planning process. In order for it to be understood across the organization, an appropriate and adequate communication program shall be implemented. The Business Risk Dictionary shall also form part of the various training programs of the Company.

Risk Champions and Risk Owners shall work together to ensure that all risks, including new and emerging ones, are included in the Business Risk Dictionary. They too shall push for the better understanding of the Business Risk Dictionary by all employees regardless of department or rank.

Oversight Structure

The ERM oversight structure of the Company is illustrated in the diagram below:

```
┌─────────────────────────────────────────┐
│           Board of Directors             │
│  ┌───────────────────────────────────┐  │
│  │ Board Audit and Risk Oversight    │  │───┐
│  │ Committee                         │  │   │
│  └───────────────────────────────────┘  │   │
└─────────────────────────────────────────┘   │
                     │                         │
┌─────────────────────────────────────────┐   │
│     President & Chief Executive Officer  │   │
└─────────────────────────────────────────┘   │
                     │                         │
              ┌──────────────────┐             │
              │  Office of the   │             │
              │  Chief Risk      │─────────────┘
              │  Officer         │
              └──────────────────┘
                     │
┌─────────────────────────────────────────┐
│ Risk Management Executive Committee      │
│ (RMEC)                                   │
└─────────────────────────────────────────┘
                     │
      ┌───────────────────────────────┐
      │ Heads of subsidiaries,        │
      │ business units, projects      │
      ├───────────────────────────────┤
      │ Risk                          │
      │ Owners                        │
      ├───────────────────────────────┤
      │ Risk Agents (All Employees)   │
      └───────────────────────────────┘

┌─────────────────────────────────────────────────┐
│                 Internal Audit                   │
└─────────────────────────────────────────────────┘
```
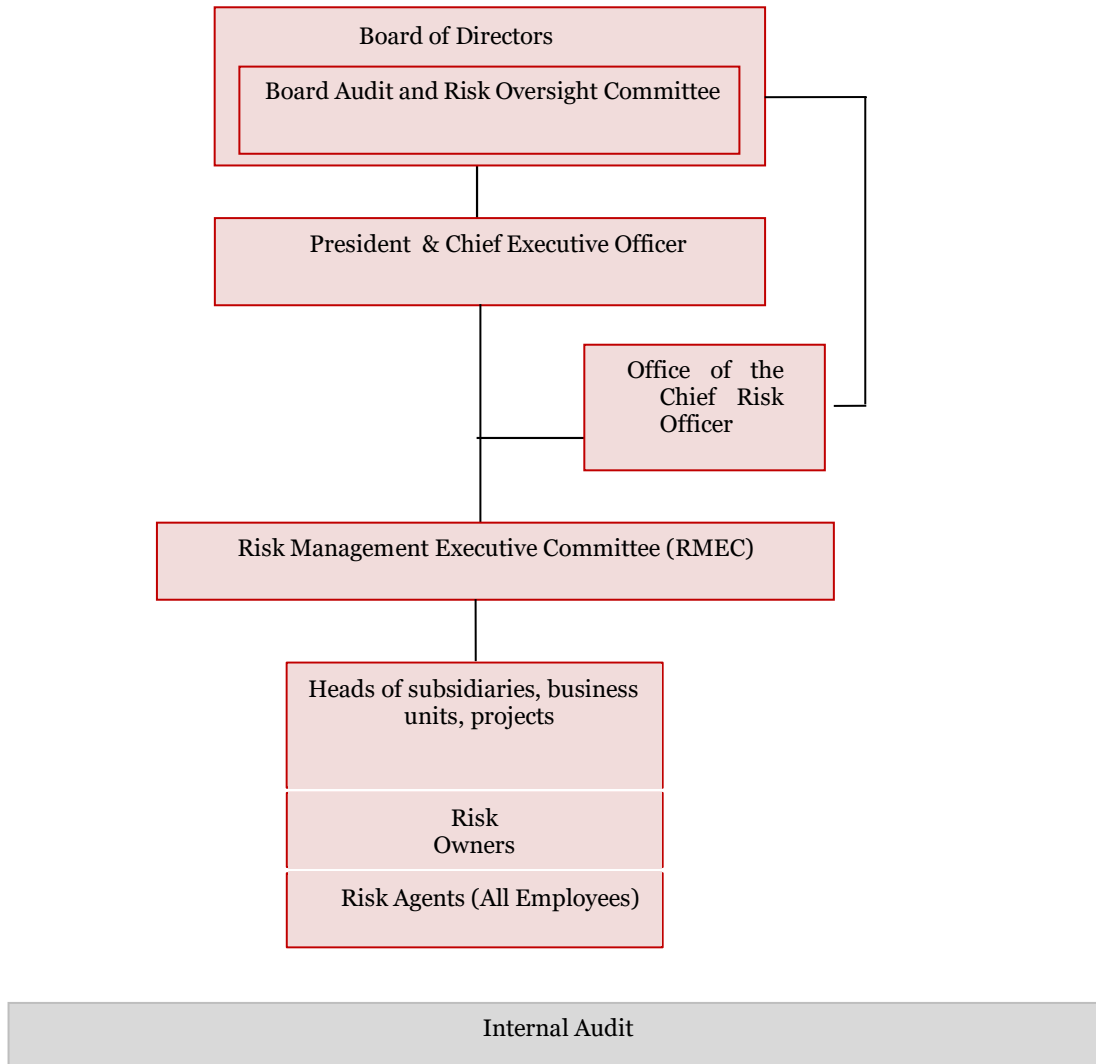
The key roles and responsibilities that are necessary to ensure effective ERM are summarized as follows:

Group/Individual	Responsibilities
Board of Directors (Board)	Provides an oversight role to risk management activities including the periodic review and approval of the ERM Policy, ERM Framework and ERM Process through the Audit and Risk Oversight Committee.

Audit and Risk Oversight Committee (AROC)	Assists the Board in fulfilling its responsibility for oversight of the Group's risk management activities.

Group/Individual	Responsibilities
President & Chief Executive Officer	Is the overall/comprehensive ERM executive; final enforcer of ERM strategies; heads the Risk Management Executive Committee.
Risk Management Executive Committee (RMEC)	ERM think tank; defines risk priorities, aligning risk policies and strategies with overall company plan.
Chief Risk Officer	The champion of ERM at the Company; develops, implements risk management process, tools and methodologies; analyzes, develops and executes policies and reports risks; submits risk report to the Board; assesses company risk profiles.
Heads of subsidiaries, business units, projects	Business risk champions; supports the RMEC in cascading the program to the various functional groups/business units and in assessing and reporting risks.
Risk Owners	Have the overall accountability for and ownership of the assigned risks and other risks in his functional areas of responsibility; manage risks at source.
Risk Agents (All Employees)	Must regard risk management as part of their everyday activities; report emerging risks/opportunities to business risk champion.
Internal Audit	Provides independent assessment of the ERM framework on a corporate-wide basis; review compliance and assurance.

Implementing Risk Management

The Chief Risk Officer (CRO) leads the implementation of the Company's ERM Program. Appropriate timing and strategy for implementation was determined. The CRO develops the plan to ensure that risk management is applied at all levels and functions and that decision-making and target-setting are aligned with the outcomes of the risk management process.

Each Business Group or line management should ensure that it adheres to the following:

- o   Hold the Business Group Head and line management accountable for the management of risks that are significant to the fulfillment of business objectives;

- o   Set appropriate goals, objectives, targets and performance indicators for all operations to ensure that risks are effectively managed under the set ERM Framework;

- o   Allocate adequate financial and human resource for risk management consistent with corporate priorities, and;

- o   Ensure that employees at all levels within their group have the competence and responsibility through selection, education, and training to carry out the ERM process.

Monitoring and Review of the ERM Framework

The implementation of the ERM Program shall be assessed by the Internal Audit Department annually using an ERM Maturity Assessment Questionnaire. The Questionnaire considers certain criteria to determine the level of the organization's maturity in implementing the ERM Program. The criteria are grouped into components which are critical in ensuring successful implementation of the program, namely, governance and organization, risk management strategy, reporting and communication structure, tools and technology and the Company's culture and capability.

## Continuous Improvement of the ERM Framework

The ERM Framework, Process, and Plan shall be reviewed and improved periodically, taking into consideration the Company's internal and external environment at each period. The results of the assessment by the Internal Audit Department shall also be used to determine gaps between the current and desired state of ERM maturity. Decisions shall be made on how the risk management program can be improved.

The Manual shall be updated to reflect enhancements that may be made to the program. Changes shall be communicated to all stakeholders concerned.

III. THE ERM PROCESS

The ERM Process

The Megawide ERM Process is customized to Megawide Group's and individual business units' operating environment (see diagram below) and is also aligned with ISO 31000:2018. At each stage of the risk management process, tools and techniques that are suited to Megawide's and the Group's objectives, resources and capabilities shall be employed. Some of these tools are explained in detail in Chapter 4 of this Manual so that risk practitioners may choose the tool or technique that they deem appropriate in a given situation.
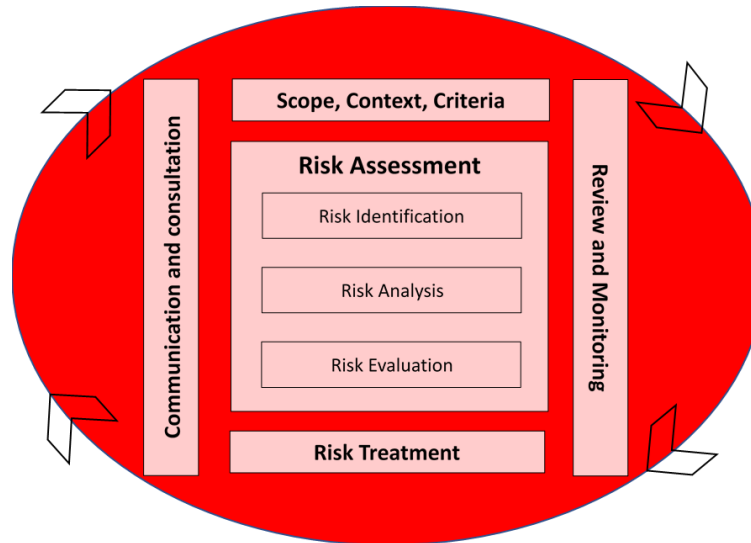
Although the process is often presented as sequential, in practice it is iterative.

Establishing the Scope, Context, and Criteria

The Company shall define the scope of its risk management activities. The scope of risk management would be every level of management activity, and all strategic planning and decision-making processes within the Company to support achievement of strategies and objectives.

Establishing the Context involves defining and understanding the internal and external parameters to be considered when managing risk. The objectives, strategies, scope, and parameters of the activities of the organization, or those parts of the organization where the risk management process is being applied, should be established. These parameters or factors will help ensure that the risk management approach adopted is appropriate.

The Context of the risk management process varies according to the needs of the organization and circumstances upon which risk management process is applied. Establishing the Context may involve defining the scope and objectives of the activity, defining the relationships that will be affected, determining liabilities and obligation connected with the activity, as well as the resources required. The Context must be properly established, otherwise, results of assessment could be inaccurate or inadequate.

The Company reviews on an annual basis the risk appetite (the amount and type of risks that it may or may not take, in relation to its objectives) that is being presented during the annual strategic planning.

Risk Assessment

Risk Assessment is the overall process of risk identification, risk analysis, and risk evaluation.

- o **Risk identification** – process of finding, recognizing and describing risk.

  The first part of Risk Assessment is Risk Identification, which is the identification of events, consequences, or changes in circumstances that could affect objectives, strategies, process, or operations. This aims to generate a comprehensive list of risks that might create, enhance, prevent, degrade, accelerate, delay, or otherwise affect the achievement of objectives. It is recognized that comprehensive identification is critical because a risk that is not identified at this stage will not be included in further analysis. This step essentially aims to answer the question: *What circumstances or events might affect the achievement of the objectives?*

  The Company adopts the ISO definition of Risk which is "*the effect of uncertainty on objectives.*" The effect may be positive, negative, or a deviation from the expected. Also, a risk is often described by an event, a change in circumstances, or a consequence.

  The organization should use Risk Identification techniques that are suited to its culture and capability. To facilitate enterprise risk identification, the Company shall developed and update a Business Risk Dictionary that serves as a checklist of possible risks. The risks in the Business Risk Dictionary shall be classified into the following:

  - **Strategic Risks** – These risks arise when there are forces in the external environment that could either put the organization out of business, or significantly change the fundamentals that drive its overall objectives and strategies.

  - **Operations Risks** - These risks arise when operations are inefficient and ineffective in executing the organization's business model, satisfying customers, and achieving the organization's quality, cost, and time performance objectives.

  - **Compliance Risks** - These risks arise when there is noncompliance with prescribed organization policies, procedures, or laws and regulations that result in penalties, fines, etc.

  - **Financial Risks** - These risks arise when cash flows and financial risks are not managed cost effectively to maximize cash availability, reduce uncertainty of currency, interest rate, credit and other financial risks, or move cash funds quickly and without loss of value to wherever they are needed most.

  It should be emphasized that the Business Risk Dictionary is intended only to be a guide to risk identification. Risk definition may be revised to better reflect the context under which risk identification is done.

- o **Risk Analysis** – process to comprehend the nature of risk and to determine the level of risk.

  The next step in the risk management process is Risk Analysis, which means developing a thorough understanding of each risk. This step involves consideration of the causes and sources of risks, their consequences or impact, the likelihood of the impact, and the effectiveness by which the risks are managed. Qualitative and quantitative analysis of the risk shall be done in order to come up with risk ratings upon which priority risks will be determined. Risk analysis shall provide an input to risk evaluation as well as to decisions on whether risks are to be treated and on the most appropriate risk treatment strategies.

  The Company uses a Risk Assessment Criteria Matrix in analyzing and evaluating risks. This matrix was designed primarily for enterprise risk management, but may be used by subsidiaries and

functional groups in other levels of risk assessment. A similar matrix may be developed for each function.

- o **Risk Evaluation** – process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or magnitude is acceptable or tolerable.

  The final step in Risk Assessment is Risk Evaluation, which involves comparing the level of risk found during the analysis process with established risk criteria. Based on this comparison, the need for treatment, further analysis, and other alternative actions may be considered.

  Part of the Company's RACM is the Risk Profile Map / Heat Map which also facilitates Risk Evaluation. Based from the matrix, Critical, High ,and Medium risks are unacceptable, hence must be treated.

Risk Treatment

Risk Evaluation might show that certain risks need to be modified. In such case, Risk Owners shall develop strategies and implement actions that will treat or modify these risks. This step is called Risk Treatment.

Appropriate risk treatment options shall be selected by balancing the costs that are required and the benefits that can be derived from implementation. It is emphasized that only risks that are not acceptable should be treated. Risks that are at a tolerable or an acceptable level should not be treated, meaning that no action is needed on such risks, but that they should only be monitored. Moreover, it is worthy to note that Risk Treatment may introduce risks. These new set of risk must be taken into consideration in selecting the appropriate treatment option.

To make ensure that risk treatment strategies are sound, complete, and realistic, they must be cross-checked against the strategies of other departments and must be consistent and aligned with corporate goals, strategies, culture, and policies. Strategies should be stress-tested in order to determine their effectiveness. This involves determining the outcome under both aggressive and conservative scenarios.

Communication and Consultation

Communication and Consultation with external and internal stakeholders shall take place at every stage of the risk management process. This will ensure accountability for those implementing the risk management process and improve the understanding of stakeholders.

The twin process of Communication and Consultation begins with the identification of stakeholders, both internal and external. A stakeholder is any person affected or benefited by the conduct of an activity.

Holding group or team meeting is one of the most common methods of communicating with, and consulting stakeholders. Interviews, email exchanges, and phone conversations may also be done.

Review and Monitoring

Like Communication and Consultation, Review and Monitoring must also be done at each stage of the risk management process. Responsibilities for review and monitoring as well as frequency and scope, should be determined. The results of review and monitoring must be recorded and reported internally and externally as appropriate.

The Company has a template for risk assessment. It contains information that is essential in monitoring and reviewing the risk. The template is scalable, and can be modified to reflect the complexity of risk assessment required by the given situation.