Risk Management Manual

Energy Absolute Public Company Limited

Preface

Energy Absolute Public Company Limited recognized risk management as a tool to increase achievement of designated objectives efficiently and effectively. Effective and efficient risk management will reduce harmful opportunity and increase value added opportunity to the company including our stakeholders i.e. shareholders.

Company's risk management committee adheres to the Committee of Sponsoring Organizations of the Tread way Commission (COSO) guidelines. The company has been applied it for risk management at appropriate or acceptable level.

Hence, company's risk management manual was prepared to be guidelines for all personnel to understand the important of risk management and be able to perform it regularly as a culture of the company. As a result, it will be a sustained increase value added to the company and all stakeholders.

Energy Absolute Public Company Limited

ACM.....

(Chainan Thumasujarit)

Chairman of Risk Management Committee

Index

Risk Management Policy

Energy Absolute Public Company Limited ("the Company") recognizes the importance of risk management as a part of good corporate governance and a significant foundation to bring the Company toward the achievements of expected objectives. Proper risk identification and management will support good decision making and enable the Company to perceive opportunities and be aware of any possible impacts on its operation.

The Company has put in place organization risk management covering risk identification, risk assessment, determination of risk management plan, as well as monitoring and management of key risks in overall to ensure efficiency and effectiveness of its risk management. The company's risk management framework covers major risks which are divided into 3 levels as follows;

1. Strategic Risk
2. Preventable Risks: Major risks that are categorized as normal risks in business operations as follows:
    - Operational Risk
    - Financial Risk
    - Compliance Risk
    - Information Technology Risk
    - Risks related to organizational structure
3. External Risks

In the implementation of risk management, the Board of Directors appointed Risk Management Committee by electing from directors or executives or qualified persons. The Risk Management Committee is responsible for followings:

- set risk management policies, supervise and support efficient risk management covering the business operations of the Company, which includes the risk of corruption, and considering and reviewing various measures to prevent those risks to be at an acceptable risk level.
- follow up the implementation, review the report of risk management to ensure the appropriateness and sufficiency of the risk management, the risk management remains in the acceptable level, and risk management has been continuously applied.

- regularly coordinate with the Audit Committee by exchanging knowledge and information regarding risks and internal control which impacts or may impact the Company.
- Encourage to have culture of risk management and proper internal control.

The Risk Management Committee has prepared risk management manual so that the Risk Management Working Group will understand the risk assessment guidelines and perform risk monitoring, status report, and consistent review of the adequacy and efficiency of risk management measures to assure of the Company's timely and appropriate risk management.

The Risk Management Working Group shall report risk status to the Risk Management Committee on a regular basis. In case of an incident that has significant impact on the Company's operation, the Risk Management Working Group shall immediately report such incident to top executives and Chairman of the Risk Management Committee. Meanwhile, risk management culture shall also be fostered constantly among the management and the employees.

Risk Identifications

In the process of risk identification, the risk management team should focus on identifying risks the organization is facing as much as possible. The commonly used risk identification methods are as follows:

1) Using the assessor's experience by analyzing the likelihood of risk from collecting information about problems/errors in work processes that have occurred in the past that have been recorded which can be used as a guideline and as preliminary information.
2) Using Work Procedure Manual to sequence the steps of the work procedures and consider each steps where events may occur and cause error or interruption to that activity or may lead to damages.
3) Brainstorming from employees or involved parties in such activities inclusive of inside and outside the organization in order to consider together of any events occurred that have a negative impact on assigned tasks.
4) Using questionnaires to those in charge of various activities whether they have any problems, errors, or risks of any kind and how such risks caused damages. However, inquiries should be made to those directly involved who truly knows various information. In addition, the answers received may not be all facts that answers may include personal opinions, feelings, and attitudes. Therefore, the assessors should use other methods concurrently.

5) Using checklists enables executives and employees in departments to review work procedures and standards according to checklist that can be prepared by themselves. In addition, they should determine evaluation timeframe within the department with a clear checklist, such as every 3 months, 6 months, or 12 months.

In this regard, the identification of risks and causes of risks should cover the following matters:

1) Damages or events that may have a negative impacts on the organization.
2) Uncertainties that may affect the achievement of organization strategies and objectives.
3) An event that may cause the organization to lose the opportunity to generate revenue or create business opportunities or recognition from external parties.
4) Risks that may occur in all aspects, such as risks in strategy, finance, personnel, operations, reputation, laws, taxes, work systems, and environment, etc.
5) Risks that may arise from both internal and external factors.

Risk Assessment

Risk assessment is a process after the organization has identified the risks. The risk assessment consists of two dimensions: likelihood and impact which the risk assessment should provide a comprehensive assessment of the basic risks according to the type of risk. Therefore, in risk assessment the assessor should identify nature of the risk from the damage that may affect the achievement of the organization's objectives in order to determine appropriate risk control measures in the future.

Likelihood is determined by the frequency of occurrences of events that caused losses which can be categorized as very low, low, medium, high and very high or the percentage of probability that it will happen considering the nature of that risk. However, estimating losses that were not so frequent in the past can be difficult. Therefore, historical data should not be used solely for reference but the organization risk factor by assessing the frequency of risks that will occur in the future should be used together.

Impact can be recognized from the severity or the magnitude of the damage when the event occurred. Assessing the severity of a loss is a projection of the amount of loss when a disaster occurs based on many factors to be considered together. Those are monetary factor, such as previous loss value, amount of loss that an organization can endure without causing disruption, and non-monetary factor such as reputation, image etc. which can be categorized as very low, low, medium, high and very high.

Degree of Risk means status of risk obtained from the assessment of opportunities and impact of each risk factor divided into 5 levels of risk: very low risk, low risk, medium risk, high risk, and very high risk.

Risk assessment can be done in term of qualitative and quantitative and can be assessed from the organization level to the department level. The assessment should cover both inherent risks and residual risks. In addition, a risk map should be made by including various related risks wherewith an event may pose a number of risks.

Risk assessment consists of a 3-step process:

1) **Determination of risk assessment criteria.**

In risk assessment, risk rating scales must be established as a standard which will be used in the risk assessment of each department, and as a step that the Risk Management Committee or the risk management working group should be working together across the organization. The 2-dimensional risk assessment criteria are likelihood of risk and degree of impact that are important to determine the degree of risk for each event which can be defined in both quantitative and qualitative criteria as the following examples:

Example: level of likelihood is defined into 5 levels of criteria as follows:

Likelihood Level (Example)		
Level	**Likelihood level**	**Description**
5	Very High	Once / 6 months
4	High	Once / >6 months to 1 year
3	Medium	Once />1-5 year
2	Low	Once / >5-10 year
1	Very Low	Once / > 10 years

Example: level of severity of the impact is defined in 5 levels as follows:

Impact Level (Example)		
Level	**Impact on Assets**	**Description**
5	Very High	Value of Damage is Greater than 50 million baht.
4	High	Value of Damage > 10 - 50 million baht.
3	Medium	Value of Damage > 5 - 10 million baht.
2	Low	Value of Damage > 1 - 5 million baht.
1	Very Low	Value of Damage > 1 million baht.

Example of determining the level of impact in 4 aspects

1. Example: Financial Impact Severity Assessment

Level	Financial Impact	Description
5	Very High	More than 3% of estimated revenue of the fiscal year
4	High	More than 2 - 3% estimated revenue of the fiscal year
3	Medium	More than 1 - 2% estimated revenue of the fiscal year
2	Low	More than 0.5 - 1% estimated revenue of the fiscal year
1	Very Low	Less than/Equal to 0.5% estimated revenue of the fiscal year

2. Example: Operational Impact Severity Assessment

Level	Operational Impact	Description			
		Operation Delays	Or	Underachieved Performance Target	Or Duration of System Interruption
5	Very High	More than 20% of Sevice Level Agreement		More than 20% underachieved	More than 24 Hours
4	High	16 – 20% of Sevice Level Agreement		16 – 20% underachieved	12 – 24 Hours
3	Medium	11 – 15% of Sevice Level Agreement		11 – 15% underachieved	6 – 12 Hours

2	Low	6 – 10% of Sevice Level Agreement	6 -10% underachieved	1 – 6 Hours
1	Very Low	less than 5% of Sevice Level Agreement	Not over 5% underachieved	Less Than 1 Hours

3. Example: Image Impact Severity Assessment

Level	**Image Impact**	**Description**			
		being sued/complained	Or **News / Publishing**	Or **User Satisfaction**	
5	Very High	Court Lawsuit and guilty	Television/Newspaper Headlines /Social Networks	Less than 50% satisfaction	
4	High	Court Lawsuit	Television/Newspaper/Social Networks	More than 50 – 60% satisfaction	
3	Medium	Publicize	News between division/ Web board	More than 60 – 70% satisfaction	
2	Low	Internal Organization	Department news/ Web board	More than 70 – 80% satisfaction	
1	Very Low	Within Department	Department News	More than 80% satisfaction	

4. Example: Personnel Impact Severity Assessment

ระดับ	**Personnel**	**Description**
5	Very High	Fatal
4	High	Serious Injury/Disability
3	Medium	Hospitalization Injuries
2	Low	Minor injury/affects health
1	Very Low	Troubled, annoyed, time wasting/ no effect

2) Risk Prioritization

When the person responsible for risk management of each department has set the risk assessment criteria from the likelihood and impact analysis of the risk factors, the next step is to rank the severity of each risk factor by using the risk assessment matrix to assess the overall risk level and determine appropriate risk control measures.

* Remarks: The Company does not use multiplication to rank the severity of each risk factor.

Risk Assessment Matrix

Risk Assessment Matrix			Likelihood				
			Very Low	Low	Medium	High	Very High
			1	2	3	4	5
Impact	Very High	5					
	High	4					
	Medium	3					
	Low	2					
	Very Low	1					

Description table of risk management according to the level of the company's risk.

Risk Level	Color Represent	Risk Description
Very High		Risk Level that significantly exceeds the level of organization risk appetite with urgent risk mitigation required.
High		Unacceptable risk level that require immediate risk mitigation to an acceptable level.
Medium		Acceptable level but must be vigilant. Internal control may be implemented for more efficient.

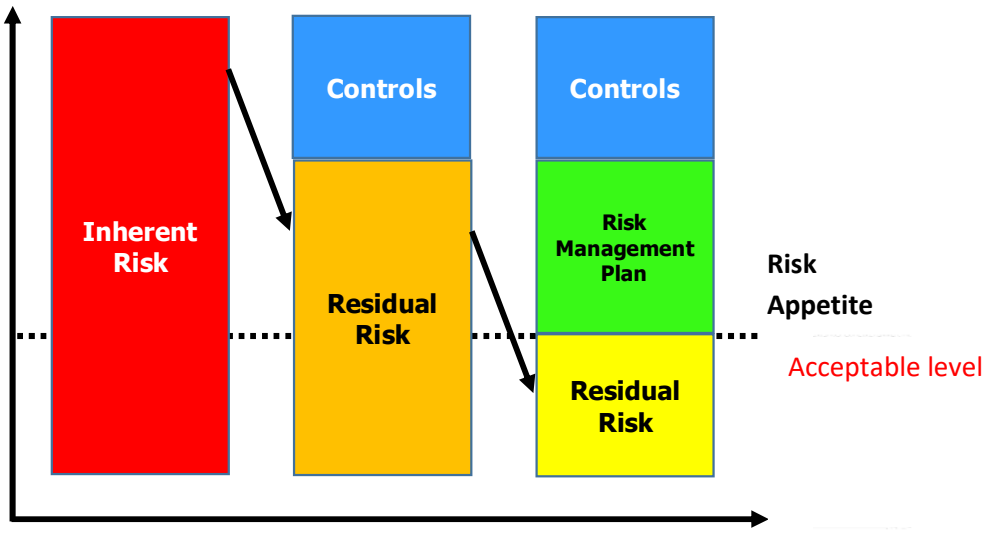
3) Assessment of existing risk control measures

After ranking the severity of each risk factor, the next step is to assess existing controls to determine residual risk which will be the starting point for defining risk appetite level for the organization. Reasons for assessing existing control measures are to be aware whether the risk level of each risk factor is higher than the existing control score or not by considering the following equation.

Residual risk = Inherent risk - Control measures

Residual risk can be reduced by increasing the level of control measures to be more efficient and effective control or by avoiding activities or businesses that cause such risks. From the above equation, the organization can determine the level of risk (Risk Score) and control level (Control Score) appropriately.

Once the risk control measures have been assessed, and if the considered risk factors can be processed under acknowledgment of senior management and allocated budget, the risk management plan can be laid out to prevent/reduce involved risks of task or project further on.



The diagram shows the relationship between inherent risk, control measures, and residual risk

Risk Management

- **Take – Risk Acceptant:** In case that risk is at an acceptable level which may not require a plan to manage that risk but must be reasonable.
- **Treat – Risk Reduction/ Risk Control:** Finding control activities to reduce risks, such as designing internal control system, work improvements to prevent or limit the impact.
- **Reduce Likelihood:** It is a risk control measure that manages factors that cause direct damage by focusing on reducing the likelihood of that events.
- **Reduce Impact:** It is a measure of risk management aim to reduce amount of damage that already occurred. It is suitable for external risk that difficult to control. The assess unit may use method of distribution of risks or diversification.
- **Terminate – Risk Avoidance:** It is a decision not to get involved with that risk situation or terminate activities that cause risks.
- **Transfer –Risk Sharing/Risk Transfer**: It is the transfer of responsibility or burden of loss to another person or other parties to manage instead.

Monitoring and Evaluation

For highest efficiency and effectiveness of risk management mechanism, there should be an arrangement of continuous and regular monitoring system. It is a cycle of evaluation that every units should know and be able to manage according to indicated time frame of monitoring such as every month, every three months or at the end of fiscal year by forming a clear risk situation reporting system, including frequency of monitoring and reporting, report format, and methods of presentation to executives. In addition, it should be set to have Exception Reports for special events such as a rare event but have high impact and significance.

Important Objectives of Monitoring are to:

(1) Evaluate quality and suitability of risk management

(2) Monitor results of risk management that already done or on going whether they achieve objectives of risk management or not.

(3) Examine progress of other control measures whether they could reduce a chance or impact of risk event to level of acceptable or not.

For monitoring, risk management report could be a tool for formal monitoring as departments be able to manage risks according to effective risk management plan, and consider to improve the defected risk management plan. Furthermore, each department may do special monitoring report to use within the department such as checklist for each section and indicate frequency for self-monitoring, which is informal monitoring. There are two formats of organization monitoring as following:

(1) Formal monitoring performs several times according to time frame setting such as every month, every three months, or every fiscal year by using company's form and report format.

(2) Informal monitoring performs during on duty, which monitor activities of each department on daily basis such as planning, checking cash, and checking reports by manager.