Module 4

FRAMEWORK OF RISK MANAGEMENT
This document is intended to be available only to the persons entitled to receive the confidential information and legal privileges it may contain.

The copyright of this document is owned by ERMA. Any duplication, reproduction, or modification in any form, in whole or in part, without prior written consent of ERMA is strictly prohibited.

We thank you for your understanding.
The EBA reading material series is consisted of the following modules:

1 - Introduction to ERM
2 - Introduction to ISO 31000
3 - Principles of Risk Management
4 - Framework of Risk Management
5 - Process of Risk Management
6 - ISO 31000 Glossary

We strongly recommend you to read the complete ERMA EBA reading material series to prepare yourself for the EBA you are participating in.
Module 4

FRAMEWORK OF RISK MANAGEMENT
Framework of Risk Management

ISO 31000 says

The success of risk management will depend on the effectiveness of the management framework providing the foundations and arrangements that will embed it throughout the organization at all levels. The framework assists in managing risks effectively through the application of the risk management process at varying levels and within specific contexts of the organization. The framework ensures that information about risk derived from the risk management process is adequately reported and used as a basis for decision making and accountability at all relevant organizational levels.

The framework consists of **five components**:

- **Component One**: Mandate and commitment
- **Component Two**: Design of framework for managing risk
- **Component Three**: Implementing risk management
- **Component Four**: Monitoring and review of the framework
- **Component Five**: Continual improvement of the framework
Framework of Risk Management

The way in which those five components interrelate in an iterative manner is shown in the figure below:

ISO31000 says further that the framework as illustrated in the figure above is not intended to prescribe a management system, but rather to assist the organization to integrate risk management into its overall management system. Therefore, organizations should adapt the components of the framework to their specific needs.

Each component is described in the following section.
Component One:

Mandate and Commitment

ISO 31000 says:

The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organization, as well as strategic and rigorous planning to achieve commitment at all levels.

In that regards, the followings are the duties of management:

- Define and endorse the risk management policy;
- Ensure that the organization’s culture and risk management policy are aligned;
- Determine risk management performance indicators that align with performance indicators of the organization;
- Align risk management objectives with the objectives and strategies of the organization;
- Ensure legal and regulatory compliance;
- Assign accountabilities and responsibilities at appropriate levels within the organization;
- Ensure that the necessary resources are allocated to risk management; communicate the benefits of risk management to all stakeholders; and
- Ensure that the framework for managing risk continues to remain appropriate.
Component One: Mandate and Commitment

In other words:

Your company’s highest governance organs such as company’s board of directors and or senior management must make a commitment to risk management. It means the management of your organization must:

- Define your organization’s risk management policy.
- Establish risk management performance indicators.
- Formulate risk management objectives.
- Assign risk management responsibilities.
- Allocate risk management resources.
- Communicate risk management benefits.
- Support your risk management framework

In implementing the standard prescribed in this clause, we must carefully observe the corporate governance practices that vary between countries, especially regarding the corporate board system.

There are countries that have a one-tier board system such as United States of America, United Kingdom, Australia, Canada, Malaysia, Singapore and India and there are others that have a two-tier board system such as Germany, French, Netherlands, Japan, and Indonesia. Countries that adopt one-tier board system are countries which use common law or anglo-saxon as the basis for their corporate law, whereas countries that adopt two-tier board system are countries which use continental law as the basis for their corporate law.

Sometimes one-tier board system is also called as unitary board or single board system, and two-tier board system is also called as dual board or two-board system. Under one-tier board system, all directors - both executive directors as well as non-executive directors - form one board. Under two-tier board system, there is the management board consisting of all executive directors and there is a separate supervisory board consisting of all non-executive directors.
Component One: Mandate and Commitment

Which system is more effective from the perspective of gaining mandate and commitment to implement integrated corporate risk management? ISO31000 doesn't say or suggest any particular type of board system as preference.

What is more important and critical is to understand from whom you must gain mandate and commitment. If your organization under one-tier board system, then the mandate and commitment must come from the company’s board of directors and its senior officers who leads day-to-day management. If your organization under two-tier board system, then the mandate and commitment must come from both the company’s management board and the company’s supervisory board.
Component Two:

Design of Framework for Managing Risk

The component of design of framework for managing risk has seven sub-components as follow:

1. Understanding of the organization and its context
2. Establishing risk management policy
3. Accountability
4. Integration into organizational business process
5. Resources
6. Establishing internal communication and reporting mechanisms
7. Establishing external communication and reporting mechanisms

Sub-component 1:
Understanding of the organization and its context

ISO31000 says:

Before starting the design and implementation of the framework for managing risk, it is important to evaluate and understand both the external and internal context of the organization, since these can significantly influence the design of the framework. Evaluating the organization’s external context may include, but is not limited to:

- The social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- Key drivers and trends having impact on the objectives of the organization; and
- Relationships with, and perceptions and values of, external stakeholders.
Component Two: Design of Framework for Managing Risk

Evaluating the organization’s internal context may include, but is not limited to:
- Governance, organizational structure, roles and accountabilities;
- Policies, objectives, and the strategies that are in place to achieve them;
- Capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- Information systems, information flows and decision making processes (both formal and informal);
- Relationships with, and perceptions and values of, internal stakeholders;
- The organization’s culture;
- Standards, guidelines and models adopted by the organization; and
- The form and extent of contractual relationships.

In other words:

In order to understand your organization’s context, you must
- Evaluate and understand your organization’s external context and then use this knowledge to help design your risk management framework.
- Evaluate and understand your organization’s internal context and then use this knowledge to help design you risk management framework.

Evaluate and understand your organization’s external context means that you evaluate and understand:
- Your organization’s external environment
- Your organization’s external stakeholders
- Your organization’s external influences

Evaluate and understand your organization’s internal context means that you evaluate and understand:
- Understand your organization’s internal stakeholders
- Understand your organization’s governance.
- Understand your organization’s capabilities.
- Understand your organization’s culture.
- Understand your organization’s standards.
- Understand your organization’s contracts.
Sub-component 2: Establishing risk management policy

ISO31000 says:

The risk management policy should clearly state the organization’s objectives for, and commitment to, risk management and typically addresses the following:

- The organization’s rationale for managing risk;
- Links between the organization’s objectives and policies and the risk management policy;
- Accountabilities and responsibilities for managing risk;
- The way in which conflicting interests are dealt with;
- Commitment to make the necessary resources available to assist those accountable and responsible for managing risk;
- The way in which risk management performance will be measured and reported; and
- Commitment to review and improve the risk management policy and framework periodically and in response to an event or change in circumstances.

The risk management policy should be communicated appropriately.

In other words:

You must establish a risk management policy for your organization, and communicate that risk management policy. It means that you have to:

- Make a clear commitment to risk management.
- Define your risk management objectives.
- Explain how your policy will be implemented.
Sub-component 3:
Accountability

ISO31000 says:
The organization should ensure that there is accountability, authority and appropriate competence for managing risk, including implementing and maintaining the risk management process and ensuring the adequacy, effectiveness and efficiency of any controls. This can be facilitated by:

- Identifying risk owners that have the accountability and authority to manage risks;
- Identifying who is accountable for the development, implementation and maintenance of the framework for managing risk;
- Identifying other responsibilities of people at all levels in the organization for the risk management process;
- Establishing performance measurement and external and/or internal reporting and escalation processes; and
- Ensuring appropriate levels of recognition

In other words
You must make people accountable for managing risk. It means that you have to:

- Identify your organization’s risk owners
- Give risk owners the authority to manage risk.
- Make risk owners accountable for managing risk.
- Establish risk management performance measurement methods.
- Develop risk management reporting and escalation processes.
Sub-component 4:
Integration into organizational business process

ISO31000 says
Risk management should be embedded in all the organization’s practices and processes in a way that it is relevant, effective and efficient. The risk management process should become part of, and not separate from, those organizational processes. In particular, risk management should be embedded into the policy development, business and strategic planning and review, and change management processes.

There should be an organization-wide risk management plan to ensure that the risk management policy is implemented and that risk management is embedded in all of the organization’s practices and processes. The risk management plan can be integrated into other organizational plans, such as a strategic plan.

In other words:
You have to build risk management into your organization through:
- Making risk management an integral part of all processes and practices.
- Developing an organization-wide risk management plan
Sub-component 5: Resources

ISO31000 says:

The organization should allocate appropriate resources for risk management. Consideration should be given to the following:

- People, skills, experience and competence;
- Resources needed for each step of the risk management process;
- The organization's processes, methods and tools to be used for managing risk;
- Documented processes and procedures;
- Information and knowledge management systems; and
- Training programs.

In other words:

You must allocate appropriate resources to support your organization’s risk management activities. It means that you have to consider providing:

- People who can support your organization’s risk management activities.
- Resources needed to support each step of the risk management process.
- Information and knowledge management systems to support risk management.
- Risk management procedures and processes.
- Appropriate risk management methods and tools.
Sub-component 6: Establishing internal communication and reporting mechanisms

ISO31000 says:

The organization should establish internal communication and reporting mechanisms in order to support and encourage accountability and ownership of risk.

These mechanisms should ensure that:

- Key components of the risk management framework, and any subsequent modifications, are communicated appropriately;
- There is adequate internal reporting on the framework, its effectiveness and the outcomes;
- Relevant information derived from the application of risk management is available at appropriate levels and times; and
- There are processes for consultation with internal stakeholders.

These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information.

In other words:

You must establish internal communication mechanisms that include:

- Internal risk management communication and reporting mechanisms
- Internal risk management communication and reporting processes
Sub-component 7: Establishing external communication and reporting mechanisms

ISO31000 says:

The organization should develop and implement a plan as to how it will communicate with external stakeholders. This should involve:

- Engaging appropriate external stakeholders and ensuring an effective exchange of information;
- External reporting to comply with legal, regulatory, and governance requirements;
- Providing feedback and reporting on communication and consultation;
- Using communication to build confidence in the organization; and
- Communicating with stakeholders in the event of a crisis or contingency.

These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information.

In other words:

You must develop an external communication plan that:

- Describes how you intend to communicate with your organization’s external stakeholders.
- Describes how you implement your external risk management communication plan.
Component Three:
Implementing Risk Management

ISO31000 says:

In implementing the organization’s framework for managing risk, the organization should:

- Define the appropriate timing and strategy for implementing the framework;
- Apply the risk management policy and process to the organizational processes;
- Comply with legal and regulatory requirements;
- Ensure that decision making, including the development and setting of objectives, is aligned with the Outcomes of risk management processes;
- Hold information and training sessions; and
- Communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.

ISO31000 says

further that risk management should be implemented by ensuring that the risk management process is applied through a risk management plan at all relevant levels and functions of the organization as part of its practices and processes.

In other words:

In implementing your approach to risk management, you have to implement both your risk management framework and your risk management process.
Component Three: Implementing Risk Management

To implement your risk management framework, it means that you have to:
- Develop a strategy to implement your organization’s risk management framework;
- Implement your organization’s risk management framework as per its strategy and approach.

To implement your risk management process, it means that you have to:
- Develop a plan that explains how you intend to apply your organization’s risk management process as per part 3 of ISO31000 anatomy: Process of managing risk;
- Use your risk management plan to implement your organization’s risk management process as per part 3 of ISO31000 anatomy: Process of managing risk.
Component Four:
Monitoring and Review of The Framework

ISO31000 says:
In order to ensure that risk management is effective and continues to support organizational performance, the organization should:

- Measure risk management performance against indicators, which are periodically reviewed for appropriateness;
- Periodically measure progress against, and deviation from, the risk management plan;
- Periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context;
- Report on risk, progress with the risk management plan and how well the risk management policy is being followed; and
- Review the effectiveness of the risk management framework.

In other words:
You have to monitor your risk management framework by:

- Evaluating the ongoing effectiveness of your risk management framework;
- Preparing reports on the effectiveness of your risk management framework.
Component Five:

Monitoring and review of the framework

ISO31000 says:

Based on results of monitoring and reviews, decisions should be made on how the risk management framework, policy and plan can be improved. These decisions should lead to improvements in the organization's management of risk and its risk management culture.

In other words:

You need to improve your risk management framework over time by:

- Studying the results of your risk management monitoring and review activities; and
- Figuring out how you are going to improve your risk management framework.