ERMA

ERMA EBA
Exam-Based Assessment
READING MATERIAL SERIES

Module 1

INTRODUCTION TO ENTERPRISE RISK MANAGEMENT

www.erm-academy.org

Disclaimer

The information contained in this document is confidential, privileged, and only for the intended recipient's information and may not be used, published, modified, or redistributed without the prior written consent of ERMA.

ERMA EBA

Exam-Based Assessment

READING MATERIAL SERIES

The EBA reading material series consists 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 1

INTRODUCTION TO ENTERPRISE RISK MANAGEMENT

A. What is ERM?

Enterprise Risk Management (ERM) is the leading approach to managing and optimizing risks, enabling a company to determine how much uncertainty and risk are acceptable to an organization.

With a company-wide scope, ERM serves as a strategic analysis of risk throughout an organization, cutting across business units and departments, and considering end-to-end processes. In adopting an ERM approach, companies gain the ability to align their risk criteria to business strategy by identifying events that could jeopardize their organizations and then developing an action plan to manage them.

Furthermore, by applying ERM in conjunction with other operational elements in the current business environment, companies can accomplish many of their governance-related tasks. Specifically, ERM can help organizations:

- Identify strategic risk opportunities that, if undertaken, can facilitate achieving organizational goals.
- Provide senior management with the most up-to-date information regarding the risk that is used/may be used in the decision-making process.
- Establish co-dependency between the ERM initiative and considerations for capital market reporting disclosures and other laws and regulations.
- Align annual performance goals with risk identification and management.
- Encourage and reward upstream reporting of business-risk opportunities and challenges.

There are various ERM frameworks that a company could follow, all of which should define the essential components, suggest a common language, and provide clear guidance for enterprise risk management. Besides, each framework that is implemented should also describe an approach for identifying, analyzing, responding and monitoring risks, and opportunities facing the enterprise.

Among the more widely known frameworks and/or standard, the related ERM definitions that they promulgate are:

- The COSO ERM framework's latest version which was published in 2017 by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). It defines ERM as "culture, capabilities, and practices, integrated with strategy and execution, that organizations rely on to manage risk in creating, preserving, and realizing value."
- The ISO 31000 Risk Management Standard's latest version which was published in 2018 by the International Standard Organization (ISO). It defines the risk management process as "coordinated activities to direct and control an organization concerning risk." It also defines the risk management framework as a "set of components that provides the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization."

B. ERM Frameworks

COSO ERM framework has its own merits and legacy in the United States of America, especially after the Sarbanes-Oxley Act was in effect. It originates from COSO Internal Control Framework published in 1992, which had been used widely throughout the world by many large corporations in managing their internal control framework. Some have seen COSO ERM framework as the expansion of COSO internal control framework, a thought that deserves its standing, especially from the accounting and auditing professionals' point of view.

ISO 31000 as an International Standard, gains full acceptance in many countries and large corporations as it is practical and business-oriented. It consists of three components: the principles of managing risks, the framework of managing risk, and the process of managing risks. Therefore, ISO 31000 captures ERM as an integrated way of managing risk.

Furthermore, its universal characteristics make them applicable to any organization, public or private, large-size corporations, or small-size corporations. Also, it is not established from the urge to comply with specific regulations but to address the uncertainty of business challenges and how to deal with them. Some have seen ISO 31000's similarity with other standards developed by the AUS/NZS 4360 Risk Management Standard originating from Australia, especially in the part of the risk management process. It is correct, yet ISO 31000 is much more comprehensive, systematic, and universal.

C. The Value of ERM

There are many benefits that ERM brings to the organization. The followings are some of the most tangible value of ERM for organizations:

1. ERM increases the credit rating

A company's credit rating has become vital to an organization's financing power, which is where ERM comes into action. Starting from 2005, Standard & Poor's (S&P) has begun analyzing the industry's ERM practices and developing criteria to assess the ERM procedures.

They started with financial institutions and insurance companies, then energy companies, and presently the entire industry sector. In this regard, the ERM analysis provides insight into those companies' management capabilities and corporate governance. In evaluating the credit ratings, S&P will focus on two universal components of ERM, i.e., risk management culture and strategic risk management.

Risk management culture includes:

- Risk management organizational and governance structure;
- Roles, capabilities and accountability of risk management staff;
- Risk management communications and transparency;
- Risk management policies and metrics; and
- The influence of risk management on budgeting and management compensation.

Strategic risk management includes:

- Management’s view of the most consequential risks, including their likelihood and the potential effect on credit;
- with which top risks are identified and how often the identification is examined and updated;
- Influence of risk sensitivity on liability management and financing decisions; and
- role of risk management in strategic decision making.

2. ERM creates stronger governance and compliance

Stakeholders – especially the shareholders and regulators, are demanding greater corporate transparency and creating strong corporate governance. Moreover, those become an essential component for every business. ERM can contribute to successful compliant and effective governance, enabling companies to better understand and measure those risks that threaten strategic objectives.

Moreover, ERM provides information that helps quantify business performance, narrow the focus of controls, and streamline compliance efforts. As a part of this process, some organizations have begun to use their risk objectives to create integrated governance, risk, and compliance (GRC) framework. By establishing a GRC framework, companies will be able to set their governance and enterprise risk objective first, then use these objectives to define compliance control requirements, including a conducive corporate control environment and culture.

Furthermore, the integration of governance, risk management, compliance, and ethics can also help an organization drive its performance more effectively and efficiently. Governance establishes objectives and, at a high level, the boundaries inside which an entity must operate. Risk management helps a company to identify and address potential obstacles to achieve its objectives. Compliance management ensures that the edges are well set and that the organization conducts business within those boundaries.

Finally, a strong culture provides a safety net when controls and structures are weak, at the same time, providing an environment that helps the workforce reach its highest level of productivity.

3. ERM helps organization to identify and exploit strategic opportunities

Successful companies need a comprehensive understanding of ERM, which analyzes what risks to avoid and exploit. Companies must view risk as a potential opportunity while also understanding there are possible undesirable outcomes.

Companies' future success will depend on the ability to weigh the expected risks versus rewards on an ongoing basis. By accepting and managing risk, companies can measure the possible reward for taking on some risk. They have the ability to maximize profit and increase shareholder value by restraining some risks and exploiting others. Therefore, the risk criteria and related risk profiles should be established to meet strategic organizational objectives, and they should be promulgated throughout organizations.

D. Getting started - ERM using ISO 31000

Any entity which currently operates has some form of risk management activities in place. However, these risk management activities are often *ad hoc*, informal, and uncoordinated. Moreover, they are usually focused on operational or compliance-related risks and fail to focus on strategic and emerging risks, which affect an organization's success. As a result, they fall short of constituting a complete, robust risk management process. In addition, existing risk management activities frequently lack transparency.

The approaches described below are based on successful practices that organizations have used to develop an incremental, step-by-step methodology to start ERM. Therefore, these approaches are also valid to be used as a reference for organizations that intend to implement ERM using ISO 31000.

While this is not the only way to start an ERM initiative, this incremental approach is designed to be very adaptable, flexible, and budget-friendly. The following are two sections that can be used by organizations to get their ERM started effectively:

- Key to Success
- Initial Action Steps

D.1. Keys to Success

We start with overreaching themes to provide management with a strong foundation for an effective ERM program as they develop and tailor their specific approach to implement ERM. These themes, namely “Keys to Success”, are available for organizations to start their ERM initiatives and to provide a useful foundation for specific detailed actions. These keys also help a company’s board address some of the acknowledged barriers and resistance points to ERM adoption.

Theme 1: Support from the Top is a Necessity

In achieving successful risk management, an ERM initiative must be enterprise-wide and also viewed as an essential and strategic effort. The company boards’ support is required to get focus, resources, and attention for ERM.

Although it is not the job of the company’s board to manage the ERM activities, they should demonstrate explicit support for the ERM initiative and oversee what senior management has designed and implemented to manage top risk exposures. Thus, ERM must be enterprise-wide, understood and embraced by its personnel, and driven from the top through clear and consistent communication. Besides, it should be delivered by the company’s board to senior management and the whole organization.

The company’s board is responsible for setting the right tone for ERM and ensuring that management is devoting the proper attention and resources to ERM.

What is more, the company board needs to put an effective ERM leader in place that is widely respected across the organization and has accepted responsibility for overall ERM leadership, resources, and support to accomplish the effort.

Theme 2: Build ERM Using Incremental Steps

One perceived barrier to launching ERM is that ERM is overly complicated and requires a significant and costly effort to implement. Related to this perception, the organizations believe that they must fulfill all of the ERM components in one single attempt to work and bring any tangible value to them. As for experience, it suggests otherwise.

In practice, some organizations, especially small organizations, have achieved ERM successes by taking an incremental, step-by-step approach to enhance their risk management capabilities and provide a more enterprise-wide view over time rather than undertake one massive launch effort. They start with a simple process and build from there using incremental steps rather than trying to make a quantum leap to implement a comprehensive ERM process thoroughly. By doing so, they can:

- **Identify and implement key practices to achieve immediate, tangible results.**
  For example, they may start by completing and sharing to their board, for the first time, regarding a shortlist of enterprise-wide risks with specific action steps to address the identified risks . This initial step would be followed by a more detailed risk assessment that looks deeper into other risks the organization faces.
- **Provide an opportunity to change and further tailor ERM processes.**
  As the organization and its executives and directors expand their knowledge of ERM, they can make additional requests to broaden or deepen the organization’s risk management activities.
- **Facilitate the identification and evaluation of benefits at each step.**
  This can be an effective way to respond to another possible barrier: “What value do we derive from ERM?”

Theme 3: Focus Initially on a Small Number of Top Risks

For an organization that starts with ERM, it probably makes sense to first identify a small number of critical risks that can be managed and then evolve from this starting point. For some organizations, such an approach means retaining the initial ERM focus towards those strategic risks that are critical to the organization in achieving its strategic business objectives.

Focusing on a smaller, manageable number of key risks would also help develop related processes such as monitoring and reporting for those specific risks. This focused approach keeps the development of ERM processes simple and lends to subsequent incremental steps to expand the risk universe and ERM processes.

Another approach to keep ERM manageable is to focus initially on a few top risks in only one critical business unit. This limited focus could be used to develop fundamental risk management processes that can be expanded across the enterprise to other business units. And when dealing with much smaller organizations, it might be useful to start things off by identifying one critical risk or risk category and building ERM processes around that one risk.

Whichever specific risk approach is utilized, the critical success factor is to focus attention on a manageable number of key risks, then employ the lessons learned to identify and manage additional significant risks across the enterprise

Theme 4: Leverage Existing Resources

Another possible barrier to initiate an ERM process is the view that significant resources, including investments or outside expertise, are required to undertake an ERM project. For example, some directors or senior executives might think that they would need to hire an experienced Chief Risk Officer or make significant investments in new technologies or automated tools.

Such a viewpoint proves to be a significant barrier to the small organizations, in particular, which might have an apparent desire to move forward with ERM but have limited resources for making it happen. Many organizations have successfully entered the ERM arena by leveraging their existing risk management resources.

Organizations often discover that they have the personnel of their existing staff who have knowledge and capabilities relating to risks and risk management, which can be effectively used to start. For example, some organizations have used Chief Audit Executive or Chief Financial Officer as the catalyst to begin an ERM initiative. In other instances, organizations have appointed a management committee, sometimes supervised by Chief Finance Officer (CFO), to bring together all personnel from across the entity who collectively have sufficient knowledge of the organization’s core business model, related risks, and risk management practices to get ERM moving.

Also, most organizations start their ERM effort without investing in a specific technology or automated tools other than basic spreadsheets and word-processing capabilities.

Theme 5: Build on Existing Risk Management Activities

Any organization which currently operates has some form of risk management activities or risk related activities already in place. These might include activities such as risk assessments performed by the internal audit, insurance or compliance functions, fraud prevention or detection measures, or certain credit or treasury activities.

By leveraging, aligning, and subsequently enhancing these existing risk-related activities, the organization can achieve immediate and tangible benefits. For example, a company might implement a standard set of risk definitions or a common risk framework. Others have confirmed their risk assessment methodologies so that all areas of the organization performing a risk assessment use the same method.

Although it makes sense to build upon existing risk-related activities, it must be done recognizing that the existing actions probably do not constitute ERM. ERM requires risk management processes that ultimately are applied across the enterprise and represent an entity-wide portfolio view of risk, which is often missing from these existing functions.

Theme 6: Embed ERM into the Business Fabric of the Organization

ERM is a management process, ultimately owned by the board of directors, and involves people at every organizational level. The comprehensive nature of the ERM process and its pervasiveness across the organization and its people provide the basis for its effectiveness.

ERM cannot be viewed or implemented as a stand-alone staff function or unit outside of its core business processes. In some companies and industries, such as global banks, it is common to see a dedicated enterprise risk management unit to support the entire ERM effort, including establishing ERM policies and practices for their business units.

However, because ERM is a process, organizations may or may not decide that they require dedicated and stand-alone support for their ERM activities. Whether a risk management unit exists or not, the key to success is linking or embedding the ERM process into its core business processes and structures. For example, some organizations have expanded their strategic plans and budgeting processes to accommodate the identification and discussion of the risks related to their plans and budgets.

Theme 7: Provide Ongoing ERM Updates and Continuing Education for Directors and Senior Management

ERM practices, processes, and information continue to evolve. Thus, directors and senior executives need to ensure that they receive appropriate updates, new releases, and continuing education on ERM, including information about regulatory requirements and best practices. This information provides the directors and senior management the opportunity to update their risk management processes as they become aware of new or developing practices. This continuous improvement process is particularly crucial with the extended focus on ERM by regulators, rating agencies, and the capital market authorities.

D.2. Initial Action Steps

Building off the theme of “Keys to Success,” above, we need to plan the initial actions and steps to support the development of a tailored ERM initiative. The plan reflects some simple, basic steps for implementing ERM, including the key step of performing an initial risk assessment.

Step 1: Seek Board of Directors (BOD) and Senior Management leadership, Involvement and Oversight

The BOD and senior management set the tone for the organization’s risk culture. Their involvement, leadership, and oversight are essential for the success of any ERM effort. The BOD and senior management should agree on their initial objectives regarding ERM, its benefits, and their expectations for successful ERM.

There should be explicit agreement and alignment of the BOD’s and senior management’s expectations, timing, and expected results at a high level. That should include agreement on the resources to be made available and targets dates for the effort. The BOD should also consider the timing and level of reporting status required to monitor and oversee the ERM effort effectively.

Step 2: Select a Strong Leader to Drive the ERM Initiative

Finding a leader to lead the initial ERM project is also critical for success. BOD should identify a leader who has the appropriate attributes to direct the ERM effort. This person does not need to be a “CRO” (Chief Risk Officer).

It is often best to initially use the existing resources, such as the Chief Audit Executive or Chief Financial Officer, to commence the ERM. The leader will not necessarily be the person to lead ERM in the long term, but the person to take the initiative started and to take responsibility for advancing the organization's ERM activities to the next level.

It is critical that the risk leader, a proper senior management, should have sufficient stature with vibrant strategic and risk perspectives of the organization. Therefore, they will be viewed as a peer by other senior management members. Embedding ERM into the business foundation in the organization is necessary. Similarly, having a risk leader who can be viewed as a peer by senior management members is vital for the success of the ERM initiative.

Step 3: Establish a Management Risk Committee or Working Group

In providing an influential lining for ERM effort, an organization should consider creating a senior-level Risk Management Committee or Working Group as the vehicle through which the designated risk leader can implement the ERM initiative.

While the use of a committee or working group in addition to the risk leader can be viewed as optional, these committees have been employed by risk leaders as a practical idea to engage the right people across the organization and to ensure the success of their ERM efforts.

Ideally, such committees or working groups would include Head of Department and key business unit leaders to ensure that the organization's ERM efforts are firmly embedded within its core business activities.

Step 4: Conduct the Initial Enterprise-wide Risk Assessment & Develop an Action Plan

In many ways, this step is the heart of the initial ERM process. The focus is to understand the agreement on the organization's top risks and how they are managed. The assessment is a top-down examination of the risks that could potentially be most significant to the organization and its ability to achieve its business objectives. While any organization faces many risks, the starting point is to seize a manageable list of what are collectively seen as the most significant risks. Here, members of the risk committee or working group could help by sharing their views or identifying people in the organization who should be involved in the risk assessment.

While there is no one best approach to conduct a risk assessment, many organizations begin by obtaining a top-down view of the most critical risk exposures from key executives across the organization. That is typically accomplished by starting with a discussion of the organization's business strategy and its components, then identifying the principal risks that would impede its ability to achieve strategic objectives. Thus, an alternative is to discuss the strategy and risks of its major business units.

The organization should then consider prioritizing or ranking the risks identified. This step could be accomplished by a simple ranking of the perceived level of inherent risk or a detailed assessment of the probability and impact of each risk. Consider using a basic scale of the high, medium, and low for each inherent risk as a starting point rather than quantification or modeling. Again, during this initial assessment, many organizations find a good discussion and helpful simple classifications. As a result of some of the significant and unexpected risks that have manifested themselves lately, some organizations are expanding their impact and probability assessments to other factors. Examples of these new factors include assessing the velocity of risk or the organization's preparedness for that risk.

The organization also needs to assess its risk responses related to identified risks and develop action plans to address gaps beyond those acceptable. Typically, action plans stemming from the initial risk assessment would identify gaps in the existing risk management processes related to the risks identified and detail specific ways to address those gaps. The initial risk assessment exercise is a time to initiate discussions about the organization's risk appetite, relative to the risks identified.

Some executives find it challenging to articulate, much less discuss, their organization's risk criteria or sometimes called as risk appetite. To overcome this challenge, consider focusing initially on qualitative or narrative descriptions of the risk criteria or risk appetite, (e.g., the organization may have zero tolerance for anything related to customer or employee safety).

Management can facilitate the discussion of the risk criteria or risk appetite by identifying types of activities or products that they will or will not undertake because of the perceived risks. Alternatively, they may discuss how risk aggressive or conservative they want to be compared to their peers or competitors.

Step 5: Inventory the Existing Risk Management Practices

During the risk assessment process, the organization should also be taking an inventory of its current risk management practices to determine the areas of strength to build upon and the areas of weakness to address. The inventory becomes valuable information for management to assist in enhancing the risk management processes.

First, it enables the organization to identify gaps in its current risk management processes relative to its critical and significant risks as identified. Risk management activities are often focused on existing operations and compliance risks, as opposed to substantial external, emerging, or strategic risks. As new risks are identified in the risk assessment process, the knowledge is gained from a comprehensive inventory of existing risk management activities. It will help the organization assess the connections between existing risk management processes and the most critical enterprise-level risks so that management can determine if there are gaps in managing critical risks. Further, it assists the organization in mapping risks to underlying objectives.

Second, the inventory forms a baseline for the organization as it continues to develop and enhance its ERM processes. It helps management demonstrate progress and the benefits of ERM by serving as a point of comparison as the processes mature.

Step 6: Develop Your Initial Risk Reporting

In the future, the organization needs to develop its initial approach to risk reporting, including communication processes, target audiences, and reporting formats. Organizations should start by keeping things simple, clear, and concise. However, regardless of what specific reporting format employed, the reporting must reflect the relative importance or significance of each risk.

To this end, many organizations use simple lists in which the top risks are listed in rank order. Some others use colors or graphics in addition to that the ranking to obtain focus attention on the significant risks. Also, consider what is reporting and tracking status that you need to monitor, especially the progress of the action plan to address the gaps in risk processes or risk responses that are identified during the ERM implementation.

Step 7: Develop the Next Phase of Action Plans & Ongoing Communications

The implementation of ERM is an evolutionary process that takes time to develop. In the spirit of continual improvement, once the initial ERM action plan has been completed, the working group or risk leader should conduct a critical assessment of the accomplishments to date and develop a series of action plans for the next stage of implementation.

Following the incremental approach, the leader should identify the next steps in the ERM roll-out that will foster additional enhancements and afford tangible benefits. The completion of the initial ERM action plan is also an opportunity for the risk leader and the ERM working group to convey the status and benefits achieved to the BOD and senior management. The risk leader should also consider what types of continuing education offerings and communications should be deployed across the organization to continue strengthen its risk culture and ERM capabilities.

E. Capacity Building Toward ERM Implementation Using ISO 31000

The capacity building to implement ERM using ISO 31000 may start with building the right understandings about ERM and ISO 31000 fundamentals and acquiring some relevant competencies, hard competencies, and soft competencies for a group of people who will lead ERM implementation in the organization.

A deeper understanding of ERM using ISO 31000 could be exercised through self-study to the ISO 31000 official documents or taking a discussion with risk professionals who have experiences in implementing ERM using ISO 31000, or through systematic courses of ERM using ISO 31000. While building the appropriate competencies for a group of people who will lead the ERM implementation using ISO 31000 requires more elaborative efforts. In that regard, ERM Academy provides a template or standard of "competency matrices," hard competency, and soft competency. Those matrices can be used by the organization as a reference to build appropriate skills for people who will be involved in ERM implementation, directly or indirectly.

Once the understanding of *ISO 31000 fundamentals* has been in place – and sufficient numbers of people have the appropriate competencies, the organization may proceed with their initial steps to implement ISO 31000 as suggested in 'getting started – ERM using ISO 31000 above'.

E. Capacity Building Toward ERM Implementation Using ISO 31000

For the core team members or champions in the ERM - ISO 31000 implementation, their capacity needs to be enhanced through mastery of *'ISO 31010 Risk Assessment Techniques'* as recommended by ISO. There are 31 risk assessment techniques – qualitative, semi-quantitative, and quantitative – which must be acquired by them. The details of those techniques are well described in the complimentary documents to ISO 31000, namely ISO 31010.

At a later stage, the core team members and the internal auditors – as an independent assurance unit in the organization – need to acquire a mastery of *'Assessing the Adequacy of ERM using ISO 31000'*. For internal auditors, the knowledge and skill are critical to equip them with the appropriate competencies in conducting an independent assurance or review of ERM's adequacy in the organization.

Likewise, the core team members would have a better understanding of the required documentation obliged to be in place and available for any independent assessment or review either conducted by internal audit or other independent assurance providers.

ERMA

ERMA EBA - Reading Material Series

Module 1
INTRODUCTION TO ENTERPRISE RISK MANAGEMENT

For further information, please visit our portal at **www.erm-academy.org** send an email to **info@erm-academy.org**