ERM Insights by Carol
Carol Williams, CRM
Carol@ERMinsightsbyCarol.com
www.ERMinsightsbyCarol.com

Guide to Developing an Enterprise Risk Management Program

What is ERM? Do you need it in your organization? What are the basic steps to implementing an ERM Program? The following answers these questions and more.

1. Defining ERM

What is ERM and how is it different from traditional risk management?

All businesses conduct traditional risk management at some level. However, it is usually one-dimensional, focusing on the impact if a potential negative event were to occur. Typically, these risks are insurable and are addressed on an individual basis as needed. (Example: Worker's compensation insurance coverage for on-the-job injuries.)

Enterprise Risk Management addresses risks to the entire organization, including risks that could lead to a positive outcome, and those that are not insurable. It also addresses the cumulative effect of risks and how they impact one another, providing management with information to take proactive action and prioritize resources. ERM also works to identify previously unseen opportunities for management to seize in order to achieve the organization's objectives or mission. Using a holistic approach, ERM is not bound to specific siloes within the organization. (Example: Managing threats to achieving the organization's strategic objectives.)

Read more:

- 8 Ways Enterprise Risk Management is Different (...and Better) than Traditional Risk Management
- 8 Possible Consequences for Not Being Proactive in Risk Management

2. Needing ERM

Does every organization need ERM? There are two areas to consider when answering this question: appropriateness and necessity.

a. Determine appropriateness

ERM isn't appropriate for every organization. The way your organization is structured and the kind of business you conduct are two determining factors.

b. Determine necessity

Since all businesses conduct informal risk management in some form or another, it's important to determine if those existing processes are sufficient to meet the organization's needs and goals. Perhaps the risk efforts of the strategic planning, project management, and audit teams adequately identify risks to the organization. If leadership believes those risks are being managed appropriately, then it may be better to strengthen those processes or expand upon them without creating a formal ERM Program.

However, it should be noted that without an ERM Program, there is no unit responsible for identifying and managing risks to the entire organization, outside of the business unit siloes. Perhaps no serious risk issues have occurred to date, but without that high-level view, and a team responsible for facilitating risk identification on an ongoing basis, risks could occur at any time. Leadership should be made aware of this potential and should knowingly accept the risk if they choose to forego a formal ERM Program.

Read more:

- 2 Simple Steps to Knowing if Your Organization Needs Enterprise Risk Management
- ERM Now Formally a Factor in Credit Ratings Issued by Top Agency

3. Before You Start

a. Critical success factors

The success of the ERM Program will be dependent on the organization's willingness to do the following:

- Provide Support—Leadership must provide verbal and actionable support.
- Be Involved—The right people must be involved to provide guidance and subject matter expertise.
- Follow Through—The organization must commit to making ERM a part of the company culture.

- Dedicated Risk Team—Knowledgeable risk professionals should be responsible for managing the daily operations of the ERM Program to ensure it gets the necessary attention and support.
- Accountability for risk owners—Hold risk owners responsible for taking the appropriate actions to manage the risk to acceptable levels.

Without leadership and executive support in these five areas, the organization cannot have a successful ERM Program. If you don't have proper support, address this with your leadership before you move forward with implementing ERM. You may still be able to cultivate a positive risk culture and then roll out ERM successfully. On the other hand, it may be more appropriate to expand existing risk management processes and forego an official ERM Program, at least in the near term.

Read more:

- 4 Critical Things Organizations Must Do to Ensure an ERM Program's Success
- 4 Possible Paths Your ERM Program Can Take

Continue reading below for more specific considerations and action items.

b. Assess Your Risk Culture

Take a look around your organization and determine the quality of your risk culture – the set of behaviors, beliefs, and attitudes towards risk.

- Do employees feel empowered to raise concerns to management?
- Do managers escalate those concerns to executives?
- Do executives seek the input of employees and use that information in the risk management process?
- Is mid-management aware of how much risk the executives and board members are comfortable taking?

This type of assessment will help you in designing the ERM Program for your organization. If you answered no to these questions, you may need to cultivate a positive risk culture within the organization as part of rolling out a new ERM Program.

Read more: 5 Critical Steps to Cultivating a Positive Risk Culture

c. Build a Network

Develop a network of key individuals throughout all levels of the enterprise. You can use their insight to better understand some of the undercurrents happening within the organization. Later, you can develop this network into a group of liaisons to help identify risks and pass risk-related information back to their units.

Be sure to obtain the support of these people, as well as management. When you roll out the ERM Program, it will be extremely helpful to have supporters already in place.

Read more:

- An Enterprise Risk Management Program is NOT One-Size Fits All
- Building a Risk Intelligence Network

d. Set and Manage Expectations

Before you begin doing risk management, make sure you set proper expectations among board members, executives, management, and your organizational network. The main message you'll want to communicate is that ERM is a valuable process that matures over time. That value comes from managing risks in a way that fits the organization—not rushing through it as a check-the-box exercise.

Include these points in your messaging and conversations:

- ERM is a long-term commitment
- Some activities will be experimental in nature
- ERM takes time to be done right
- ERM is not a red-tape activity

As for the investment cost, best practices recommend a dedicated ERM team with at least one person with ERM experience. Additionally, other employees—including management and executives—will need to allocate some time to participate in ERM workshops and exercises. As for other expenditures, the ERM unit may also wish to purchase software to track risks as products like Excel are not recommended for long-term use.

The time commitment depends on the resources – primarily people and time – available to the organization. The process and timing should fit the rhythm of the organization, such as annual planning sessions and scheduled board meetings. And subject matter experts, the business people, are handling their responsibilities in addition to providing information and perspective to ERM, so the scheduling is dependent upon their calendars as well.

Read more:

- An Enterprise Risk Management Program is NOT One-Size Fits All
- 4 Critical Things Organizations Must Do to Ensure an ERM Program's Success
- Handling Unrealistic Expectations of Enterprise Risk Management

e. Leverage existing processes

Review existing management processes to identify if any can be leveraged as part of risk management. For example, if management is performing a SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis, those results can be used to identify risks. This will help you avoid duplicating efforts while showing that you value the processes of others and are able to integrate them into your workflow.

Read more: Avoid the Dreaded "Bureaucracy" in your ERM Efforts

4. Lay the Foundation

Traditional risk management is something most organizations do automatically. They avoid overly risky situations and make decisions to transfer known risks (e.g. buy insurance). These organizations make the best decisions they can in the moment, with the information at hand.

By its nature, ERM is a much more structured program. It addresses risks to the enterprise, and how those risks are identified, managed, and reported. It also establishes parameters of acceptable and unacceptable risk exposures, helping managers and executives make risk-informed decisions. This structure helps the organization charter its course and reach strategic objectives; identifying opportunities to be seized. it also creates a standard against which the organization can be audited and credit ratings can be determined.

This is why proper governance documents must be formalized before you begin performing Enterprise Risk Management.

a. ERM Framework

The ERM Framework is a high-level overview of your ERM Program that you can provide to the board and senior management. It can also be used as a reference point for auditors, credit ratings agencies, and others.

At a minimum, the ERM Framework should do the following:

1. Define ERM and establish objectives for the program
2. Provide high-level overview of risk management standard, process, etc.
3. Detail where the ERM program will reside within the organization structure
4. Assign roles and responsibilities within the organization

Since this document will be reviewed and approved by senior leadership, it should *not* provide the details of how the ERM department will function on a daily basis or the processes to be used, especially since those details will change over time.

Read more:

- Launch Your ERM Program by First Establishing Governance Structure, Principles, and Processes

- ERM and Internal Audit: The Right Relationship

b. Risk Appetite Statement

The organization's risk appetite is the amount of risk the board and senior executives are willing to take to achieve strategic objectives. The Risk Appetite Statement should define risk levels that are acceptable and unacceptable according to defined targets, ranges, floors, or ceilings.

The document that contains the risk appetite can be known as either the Risk Appetite Statement or Corporate Risk Profile.

Read more:

- Launch Your ERM Program by First Establishing Governance Structure, Principles, and Processes

- How to Use Risk Appetite and Risk Tolerance to Guide Decisions

c. Process Document

The Process Document details the methodology for the ERM Program, including how the ERM department will identify, assess, mitigate, and report risks. It is meant to be an internal guide for the ERM staff. As part of their communication efforts, the ERM

staff may wish to share the Process Document with other employees to help clarify the risk methodology and set expectations.

However, this document is too detailed—and can change too frequently—for board or executive consumption. Instead, you may wish to develop an executive-level summary of the process to share with interested executives.

Read more: Launch Your ERM Program by First Establishing Governance Structure, Principles, and Processes

d. Ensure approvals from appropriate level of management

The ERM Framework and Risk Appetite Statement will need to be approved by senior leadership and, most likely, the board of directors. To ensure executive buy-in, consult the executives as the documents are being drafted.

5. Roll out the Process

a. Typical steps in the ERM process

The basic steps in the ERM process involve the identification, assessment, management, and reporting of risks. Management, executives, and leadership use that risk information to make decisions for the organization.

These steps can be applied at any level—from risks to individual projects and processes to those that threaten strategic objectives. It is important to identify the purpose, or context, of the planned risk management activity up front to ensure you are meeting the appropriate goals.

Roles and expectations can vary depending on the step of the ERM process. Therefore, you will need to ensure clear communication with all parties involved in ERM, from executives to staff.

Read more:

- 5 Effective Risk Identification Methods eBook
- Practical Steps to Preparing and Responding to Risk Events

b. Test your process with a pilot group

No matter how well you plan, what looks good on paper may not work well for your organization. Instead of rolling out the risk process to the entire company, start with a pilot group. Try to use a business unit or process led by a manager who is a potential early adopter of the ERM Program and its goals.

Read more: Experimentation and ERM: How ERM is like Manufacturing a Product

c. Focus on Top Risks

Leadership will want to see value quickly, so start with Top Risks. These are risks that executives identify as being important to their areas and/or the organization as a whole. First, work with the executives to identify risk tolerance levels around the context (strategic plan, their area, etc.) and identify the Top Risks; then, work with their management teams to score the risks. (It is always interesting to see if these Top Risks really top the list once the scores are analyzed and compared to risk appetite.)

While many of the organization's risks will be too detailed to communicate to the board, the Top Risks list is one the board will want to keep an eye on. It should be managed carefully and communicated to all managers.

Read more:

- How to Use Risk Appetite and Risk Tolerance to Guide Decisions
- 5 Effective Risk Identification Methods eBook

d. Next Steps

Identify potential areas of integration, such as strategic and/or annual planning, project management, vendor management, or process changes. In addition to providing value to these activities, ERM may also be able to utilize some of their outputs (e.g. lists of known concerns or realized issues). Having ERM as part of these key processes can help embed ERM into the organization, which in turn matures the ERM Program overall.

Read more:

- 5 Critical Steps to Cultivating a Positive Risk Culture
- ERM as a Strategic Tool for Companies
- 3 Best Practices for Factoring Risk into Your Strategic Planning Process
- 4 Ways ERM Can Add Value During the Project Lifecycle

e. Education and Training

Partner with existing training units within your organization to ensure all executives, management, and staff are aware of their roles within the ERM process and what is expected of them within each of those roles. This is also a good way to continue cultivating a positive risk culture.

6. Modify the Program as Needed

Designing an ERM Program is like an experiment; you have to be mentally and emotionally ready to try things that may not work and make adjustments to get the best fit for your organization. If you realize something isn't working or you receive feedback from people, then adjust the process. Only by being flexible and adaptable will your ERM Program provide the most value and continue to thrive within your organization.

Read more:

- An Enterprise Risk Management Program is NOT One-Size Fits All
- How Well Does Risk Management Adapt to Changes?
- Experimentation and ERM: How ERM is like Manufacturing a Product

If you have any questions about this document or want to know more about ERM, please contact me at Carol@ERMinsightsbyCarol.com.