

Satisfying Your Risk Appetite: The Concept of ERM

[KB Website](#)

[Publications](#)

[Community Involvement](#)

[Newsletter](#)

By Jay Derr, CPA



Companies that are hungry for success review their strategic and operation objectives while addressing major risk factors to determine whether they have satisfied their risk appetite. Risk appetite is the level of risk that management is willing to accept while attempting to create value for the organization. Assessing and addressing risk is a key component to any successful business operation.

The Concept of ERM

Enterprise risk management (ERM) is an ongoing process by which senior executives consider all potential risks within the organization, both internally and externally, to determine what risks provide the greatest threats to the company. The process takes a top-down, holistic view of key risk exposures that affect the organization's ability to achieve strategic, operation, reporting, and compliance objectives. Management looks at these risk exposures and tries to determine a course of action for managing each risk.

This process helps management determine what level of risk that executives are willing to take in each area of the business to further enhance the value of the organization. Executives need to communicate the organization's strategy and goals to management, so management can properly address the risk exposures that most affect the organization's ability to achieve these objectives.

Steps in the ERM Process

1. **Identifying Risks** - The first step in the process is to brainstorm activities or scenarios that could create risk. A manager from every department should attend this meeting so that risks that affect all areas of the organization are included. Internal and external risks and past, current, or potential risks should be included in this analysis.

Risks can typically be categorized a variety of ways, including economic, industry, social, technological, political, environmental, business continuity, project, human resource, health and safety, reputational, reporting, or legal and regulatory risks.

2. **Ranking Risks** - The second step is ranking the risks by likelihood and impact. The best approach to categorizing risks is creating a portfolio view of key risks. A portfolio view is a graph that has the likelihood of an event occurring on the horizontal axis and the impact of the event on the vertical axis. This approach helps management prioritize top risk exposures based on the probability of the event occurring and the impact the event would have on the organization.

3. Addressing Risks - Once the risks are prioritized and graphed, executives must determine which events have greater risk than their desired risk appetite. These risks are analyzed further by determining what procedures are in place or need to be added to reduce their likelihood of occurring. Low impact and/or improbable risks are within the executive's risk appetite and thus can have some of their resources reallocated to greater risk areas or kept the same.

Now that the risks have been determined, the current controls that address each of these risks should be listed. If the current controls do not reduce the risk low enough to be within the executive's risk appetite, then new controls should be analyzed to determine which will provide the best benefit for the cost. If the risk is too high or new controls cannot lower the risk to a satisfactory level, the organization must decide to avoid, share, or accept the risk. An example of avoiding risk would be an investment company choosing not to invest in subprime mortgage loans because these investments are too risky.

Management should implement new controls that would lower the highest risk items to a satisfactory risk level if shareholder value is not compromised. Cost, ease of implementation, and effectiveness should be considered when making the decision to add new controls. Management should develop a plan that aligns risks with the organization's risk appetite and tolerance levels.

4. Implementing Controls - The next step is to designate an employee to oversee the implementation of new controls. Procedures are developed and implemented to ensure that the control activities are effective. The new controls are communicated to the proper employees to enable them to carry out their new responsibilities. When implementing controls, flowcharts of processes with current controls and narratives linking organization objectives with operational risk exposures and responses should be created.



5. Monitoring the Process - The final step of the ERM cycle is measuring the effect of each new control and monitoring how well it is addressing risk. Effective monitoring includes ongoing procedures and separate evaluations of how well controls are reducing risks.



Senior management assesses the effectiveness of the procedures in place and determines that the organization is maximizing its overall capabilities given staff size, budgets, and operational requirements. When applicable, internal auditors should monitor the ERM process to determine the effectiveness of procedures designed and implemented by senior management.

Since ERM is an ongoing process, these five steps should be done at least annually to adjust to any changes in an organization's internal or external environment. By continuously analyzing and addressing the risks within the organization, management can build value and reduce uncertainty.

ERM 101

1. Identify risks/brainstorm
2. Rank/prioritize
3. Address risks
4. Implement controls
5. Monitor the process

Benefits of ERM

Effective ERM processes improve organizational performance by ensuring strategic objectives are met and determining that management is responding appropriately to the most significant risks of the organization. This process also helps organizations effectively handle future events or threats by having proper controls or procedures in place to deal with uncertainty. ERM enables shareholders to assess capital needs and determine how funds should be allocated to various departments based upon their risk exposures.

ERM is conceptually designed to benefit both large and small organizations; however, large organizations have more capital and employee resources to utilize. Small organizations can use the ERM framework to determine their greatest risks and ways to control or reduce these risks to a satisfactory level. They might not be able to implement new procedures or controls because they lack the financial or human resources. In these cases, the organization should maximize their available resources to address the largest risks and may have to accept lesser risks because the cost or effectiveness of new controls doesn't outweigh the benefits.

According to a September 2008 survey of CFOs conducted by North Carolina State University faculty, only 9% of organizations have a complete formal enterprise risk management process in place. This is a small number of companies that have properly evaluated whether shareholders' risk appetite is being achieved. Organizations should set clear goals and objectives, and management should evaluate the procedures in place to determine that risk exposures do not prevent the organization from meeting its objectives.