The Governance Institute

Enterprise Risk Management Policy

Policy No.:______________
Title: Enterprise Risk Management
Policy Date:
Approval Date:

Definition

Enterprise risk management (ERM) is an ongoing strategic process that is applied systemically across the organization. It closely links the organization's strategy, operations, finance, and treasury,[1] which together define the totality of a healthcare organization's risk-bearing chassis. The ERM process is designed to identify potential events and risks that may affect the organization and to help prioritize and then manage those risks in the most appropriate manner given the organization's defined risk "appetite."

Recommended Approach

- A process of thinking about and actively managing risk across the entire enterprise in order to achieve the highest possible business success
- An optimal way of thinking about the organization's most significant risks and opportunities, matched against the organization's ability to carry such risks and achieve such opportunities
- A process used to integrate strategy, operations, finance, and treasury activities in the organization
- The "heart" of a vibrant and enterprise-wide ongoing strategic process that is applied systemically and horizontally across the organization, closely linking strategy, operations, finance, and treasury

Purpose

The board is responsible for approving and monitoring the organization's enterprise risk policy, plan, infrastructure, and framework developed by management.

Policy

The organization's ERM process and plan will:

1. **Be CEO-championed.** The CEO has direct responsibility for "driving" the approach, with engagement and approval by the board and involvement of managers across the organization.

[1] "Treasury" management is the management of the non-operating assets and liabilities of a business or organization.

2. **Be guided by an assessment of controllable and non-controllable factors**, and applied across the whole organization. Controllable factors are internal to the organization, emanating from its business activities. Examples include service line offerings, physician integration strategies, and staff compensation models. Non-controllable factors are external variables that can impact the organization independently of how it is operating its businesses, such as regulation, worldwide capital markets, and payment systems. Mapping controllable and non-controllable risk (measuring risk on a “severity of impact” and “likelihood of occurrence” grid) can provide a visual representation of identified risks in a way that easily allows ranking and prioritizing.
3. **Use a corporate finance approach *plus* scenario envisioning.** The corporate finance approach provides the quantitative discipline and specific tools needed for analytic work. Tools include a credit analysis, integrated strategic-treasury-financial plans, sensitivity analyses, financial models, and asset-liability management analyses. Scenario envisioning or planning is a forward-looking, more qualitative approach that asks the broadest possible “what if” questions.
4. **Be defined as a critical organizational success factor.** An organization’s long-term financial success will be linked to how well its leaders understand and ensure the application of ERM enterprise-wide. Accomplishing far more than helping to manage or mitigate risk, ERM guides organizations toward identifying, seizing, and achieving opportunities

Procedure

Supported by the CEO, the organization’s management team uses ERM to closely monitor risks, according to defined risk-tolerance guidelines that emerge from comprehensive assessments. The team also uses ERM to track trends and issues with strategic and financial implications, and devise and implement effective plans to address the challenges.

The board (or appropriate board committee responsible for enterprise risk) will:

1. Review the risk management plan at least once a year.
2. Define risk review activities regarding the decisions (e.g., acquisitions), initiatives (e.g., new products or service lines), and transactions and exposures (e.g., by amount) and prioritize them.
3. Oversee and assess the risk program/interactions with management and obtain regular assurance from management that all known and emerging risks are being identified and mitigated/managed to the board’s expectations.