by Julie Ryan

# The nexus between strategy and enterprise risk management

## Developing a stronger strategic plan

Strategy and enterprise risk management are often led by different groups, and used for different purposes, within companies. Strategy maps out the future for the organization. It positions the organization for success by developing clear strategic initiatives and setting out a roadmap to implement initiatives. This is done with the objectives of meeting customer needs and anticipating competitor threats. In effect, we think of strategy as creative and forward-looking. In contrast, enterprise risk management (ERM) is often described as a discipline that identifies potential risks facing the organization as well as gaps in compliance and internal controls, as a tool to audit the organization and identify failures. It is not surprising that many of us see strategy and enterprise risk management as very different; but when an organization can integrate these elements, the likelihood of success increases.


*It is not surprising that many of us see strategy and enterprise risk management as very different; but when an organization can integrate these elements, the likelihood of success increases.*

We are hearing more and more about the intersection of risk management and strategy from leading ERM organizations. COSO (Committee of Sponsoring Organizations of the Treadway Commission) may be the most widely used ERM model among U.S. companies. When COSO originally published its *Enterprise Risk Management — An Integrated Framework* in 2004, the framework was modeled closely after COSO's internal controls framework. The ERM framework includes internal environment; objective setting; event identification; risk assessment; risk response; control activities; information and communication; and monitoring. In objective setting, COSO emphasized that management needs to understand risks associated with a range of strategy choices. Furthermore, the assumed risks should be aligned with the organization's mission, vision, and strategic objectives.

A decade after the initial COSO ERM model was published, COSO solicited input from the risk management community to update the framework. In its 2014 solicitation FAQ, COSO stated, "The updated *Framework* is expected to help organizations adapt to increasing complexity and pace of change, mitigate risk to the achievement of specific strategic, operations, compliance, and reporting objectives, and provide reliable information to support sound decision-making." With this guidance, COSO was signaling that ERM can be used for far more than just improving an organization's internal controls. At the time of this writing, the new COSO Framework has not yet been released; however, the 2014 guidance hints that the revised framework will likely promote ERM as a tool for successful strategy execution through risk identification and mitigation.

Another highly respected ERM model is the International Standards Organization's (ISO) *Risk Management — Principles and Guidelines* for enterprise risk management (ISO 31000:2009). This, too, has been widely adopted among U.S. and international companies. ISO is an independent organization that is one of the world's largest developers of voluntary international standards. The ISO 31000 changed the conventional definition of risk from "chance or probability of loss" to "the effect of uncertainty on objectives." Within its 10 principles, ISO emphasizes that risk management is integral to all organizational processes; is woven into decision making; can create and protect value; and facilitates continual improvement of the organization. Simply put, ISO promotes ERM more as a culture than a tool. A strong ERM approach helps an organization meet and exceed its strategic objectives.

Another linking of risk management to strategy emerged in 2008 when Standard & Poor's first factored risk assessment in its ratings analysis. It wrote that ERM could help a firm "[avoid] situations that might result in losses

that would be outside the firm's tolerance." ERM was a method to shift management's focus from "cost/benefit" to "risk/reward." Then in its *2012 Guidance on Management and Governance*, Standard & Poor's again linked risk management to strategy and effective management of the enterprise when it wrote that the analysis of management and governance included a review of management's focus on strategic positioning, organizational effectiveness, and governance, as well as risk management/financial management.

ERM can help an organization develop and implement better strategy, and there are two practical ways to integrate risk management with strategic planning. Winston Churchill once said, "However beautiful the strategy, you should occasionally look at the results." First, the organization should review prior results and consider its ERM risk inventory when conducting a strategic situational assessment. As a company assembles its SWOT analysis of internal strengths and weaknesses, and external opportunities and threats, it can reflect upon the potential internal risks causing these weaknesses and the external risks posing threats to the organization's success. In this fashion, the risk analysis becomes part of the strategic situational assessment.

Second, an organization should review its strategy for potential risks. This can be done through "What if?" discussion and scenario analysis. The questions should consider the external landscape with attention to new customer trends, emerging technologies, evolving regulation, and the changing marketplace. What risks are our customers facing and how can we help them address those? And what are the threats to our industry or to the marketplace in which we operate? From here, mitigation planning can be undertaken to strengthen the strategic plan.

Applying effective risk management to strategic planning will help organizations identify potential pitfalls and challenges early on. Strong risk management builds credibility with stakeholders and reassures customers that the organization is proactively thinking about how to best serve them in the future. When management is willing to look critically at potential risks, it can turn them into opportunities. NWPPA

*Julie Ryan is the managing partner at Aether Advisors LLC, which advises clients on strategy and risk management. She is also director of the Utility Management Certificate Program at Willamette University in Portland, Ore., and is an instructor for NWPPA. She can be contacted at either jryan@aetheradvisors.com or (206) 329-0424.*