Article from

Risk Management

May 2019
Issue 44

Real-World COSO Implementation

By Damon Levine

The 2017 update to the Committee of Sponsoring Organizations of the Treadway Commission (COSO) guidance on enterprise risk management (ERM) frameworks ("the Guidance") stresses the importance of considering risk both in the strategy-setting process and in driving performance.[1] Figure 1, from the updated COSO Framework, describes five key components, each supported by a set of principles. The principles describe various approaches that are applicable to a wide variety of organizations. They provide management and the board with a reasonable expectation for effective risk management that is aligned with its strategy and business objectives.

Realizing COSO's theme of linking ERM to strategic objectives and execution is challenging in practice. A strength and weakness of COSO is that it is by no means prescriptive. This allows for customization of an ERM framework to company culture, sector, goals and capabilities. However, it does not offer much in the way of concrete suggestions for how an organization may achieve many of its lofty goals.

This article presents an approach that allows organizations to achieve the ERM–strategy link touted by the Guidance. We begin with an example in a real-world business objective, then illustrate how these techniques may be applied to the Guidance itself. After all, reaching an ERM maturity that meets COSO's goals is certainly a strategic objective fraught with considerable risk and uncertainty. Knowledge of these key challenges and practical countermeasures represents a risk manager's best chance of implementing a comprehensive and robust framework.

LOGICAL FRAMEWORK APPROACH

The author has previously described leveraging the Logical Framework Approach (LFA) to create buy-in for and ensure implementation of strategic risk management.[2] The following steps, inspired by LFA, begin with a clear statement of the strategic objective of interest:

1. Carefully describe the strategic objective, OBJ, for the organization (including measurable success criteria, time horizon, etc.).

2. Working with key members of the team responsible for execution, list the critical subgoals or foundational tasks necessary to achieve OBJ. Denote these subgoals as G1, G2, . . . , Gk. For convenience, we name these so we have a time-based sequence where G1 enables G2, and G2 enables G3, and so on, until Gk enables achievement of OBJ. Some find it helpful to begin by thinking of OBJ and work backward to obtain a "causal chain" of subgoals. Many projects contain tasks that are performed in parallel with the others

Figure 1
The Five Components of COSO's 2017 Guidance on Enterprise Risk Management

Source: COSO. *Enterprise Risk Management Integrating with Strategy and Performance (Executive Summary)*, June 2017. Copyright © 2017 by COSO. Used by permission. All rights reserved.

and may not have any obvious causal relations. These can simply be included within the relevant Gk based on their target completion dates.

3. Writing the sequence of subgoals from step 2 in a more streamlined format we have

$$G_1 \rightarrow G_2 \rightarrow G_3 \ldots \rightarrow G_k \rightarrow OBJ$$

where each arrow suggests that one goal's attainment enables that of the next. The arrows can be viewed as "if-then" assertions because they suggest *if* this task is completed *then* the next task may be completed. These if-then arrows make their own assumptions and come with risks and challenges. The same can be said about each of the goals: Execution comes with uncertainty.

4. Based on discussion with those team members from step 2, identify risks to achieving the subgoals $G_1, G_2, \ldots, G_k$ and necessary conditions underlying the if-then arrows from step 3.

The strategic risk analysis coming from this process leads to discussions about current and potential mitigations, with cost-benefit analysis, and risk quantification in relevant metrics (e.g., GAAP earnings impact). We now walk through a *simplified example* of the approach applied to a strategic objective of expanding distribution of a U.S.-based product to Brazil, with the goal of 2020 GAAP net earnings of (at least) 10 million USD. This statement represents our OBJ as mentioned in step 1.

To achieve OBJ the company must accomplish the following:

G_1: Obtain necessary regulatory, legal and compliance approvals;

G_2: Based on applicable laws, regulations, market environment and other factors, outline strategy for distribution, pricing, administration and so on, leveraging knowledge of U.S. operations;

G_3: Develop IT platform for sales, user interface, administration and other considerations based on above, Q3 2019; and

G_4: Train staff in use of IT platform, strategy and so on and create local presence by Q4 2019; begin sales effort in early January 2020.

So, we have the following causal chain as described in step 3:

$$G_1 \rightarrow G_2 \rightarrow G_3 \rightarrow G_4 \rightarrow OBJ$$

Step 4 is about identifying risks, challenges, success factors and other uncertainties that affect attainment of the subgoals G_1, G_2, G_3, G_4 and the required conditions for the if-then arrows to hold true in practice.

Results are summarized in Table 1.

The preceding analysis leads to a strategic risk inventory associated with the strategic objective OBJ. In addition to the risks identified in the Internal and External columns, any challenges

Table 1
Risk Analysis for Brazil Product Launch (Example)

	Risks/Uncertainties			
Subgoal	**Internal**	**External**	**Causal Link**	**Necessary Conditions***
G_1	Research and filing time constraints; inaccuracy and noncompliance	Uncertainty of application of certain regulations and potential legal changes	$G_1 \rightarrow G_2$	Strategy must conform to legal/ regulatory environment
G_2	Incorrect assessment of market/ economic conditions; product mispricing	Political uncertainties that may impact viability of strategy and consumer demand	$G_2 \rightarrow G_3$	IT platform designers must clearly understand requirements and adapt for local environment
G_3	Resource constraints that may delay IT beta and debugging efforts	Internet bandwidth/speed issues and provider pricing	$G_3 \rightarrow G_4$	Training content must be complete and robust; English to Portuguese translation will be required
G_4	Lack of effectiveness/timeliness of training	Insufficient pool of talent available; required compensation	$G_4 \rightarrow OBJ$	Sales targets and margins are met; exchange rates remain in expected corridor

* Conditions regarded as needed for indicated causal link to hold true. Factors that put these conditions in doubt should be included in the strategic risk analysis for the objective.

to or uncertainties around the necessary conditions leads to additional risks to OBJ. Using relevant metrics (e.g., GAAP earnings impact), the risks are then quantified. After consideration of any existing and potential controls and mitigations, a prioritized risk list may then be presented to management and/or the board.

Such analysis might include these factors:

- The internal risk "resource constraints may delay IT beta and debugging efforts" may need additional mitigation in the form of contract workers to assist the permanent team in some of the development and debugging efforts.

- The external risk "internet bandwidth/speed issues and provider pricing" may require very advanced planning, contract negotiation and a higher budget for these services.

- The last causal relationship, that G_4 leads to OBJ, depends in part on an expectation that a certain level of local sales and profits (in Brazilian Real) will be translated into at least 10 million USD at the foreign exchange (FX) rate then in effect. To mitigate the potential for adverse FX rates, the company may consider some type of FX hedging such as currency forwards.

In each case, a risk should be considered in terms of likelihood and its expected impact to key metrics used by management and the business line in question. Arguments for additional mitigation effort and/or investment must include a cost-benefit analysis.

COSO GETS A TASTE OF ITS OWN MEDICINE

The approach illustrated in this paper, inspired by LFA, is one path toward the strategic integration the Guidance proposes. In addition, the method provides several important insights when it is aimed at the objective of implementing an ERM framework that meets COSO's aspirations. For the sake of brevity, we use an abbreviated version of the methodology to highlight *some* of the areas of the Guidance outside of strategic risk management that are likely to be challenging.

Risk Culture

The Guidance suggests that a company defines its desired culture. Culture in an organization is, at best, a nebulous concept. It is safe to say that *risk culture* is typically less clear. It is also safe to say that the ultimate goal of the communication of risk culture would be to positively impact behavior that will lead to value creation and downside protection. One of the necessary subgoals for such an objective is that employees clearly understand their expected actions and responsibilities for risk management. Risks to achieving the objective of a pervasive, healthy risk culture include training or communication that is too broad or diluted, as well as, at the opposite end, including details that apply to only a small group of those being trained. For this reason, targeted training must be developed and might apply to each line of defense separately or can be customized for type of risk, such as operational, financial or hazard. If the notions of risk owner and mitigation owner are used as part of the ERM framework, an owner should know the expected analysis, methods, cadence, metrics and reporting requirements. Additionally, those in the first line of defense who are *not* risk or mitigation owners must have a clear understanding of how they contribute to ERM and are expected to make risk-intelligent decisions.

An additional challenge to establishing an effective risk culture is that some functional areas, departments or locations sometimes seem to get, through design or omission, a "free pass." If a definition of desired risk culture omits from its purview any specific area—new product "experiments," mergers and acquisitions, new geographies or specific functional areas such as asset management or business continuity planning—the ERM framework will likely suffer.

Further, ERM comes down to people, of course. To "attract, develop and retain capable individuals" in a risk function, there must be a budget for the department that rivals that of other critical areas. Additionally, a C-suite executive, such as a chief risk officer, should have the same influence (and compensation?) as other C-suite executives. Ideally, resources will be sufficient to have a team of full-time risk management employees. If the days of having one or two full-time risk management employees or risk being accomplished as a "favor" are not yet gone, their departure cannot come soon enough.

The ultimate goal of the communication of risk culture is to positively impact behavior that will lead to value creation and downside protection.

Risk Appetite and Strategy Selection

The aspiration to deploy enterprise risk management capabilities as part of selecting and refining a strategy comes with challenges, including (1) ERM processes for strategy design or choice that may not be nimble enough to move at the "speed of business," (2) ERM that is not viewed as a natural strategic partner and does have a seat at the table for such discussions and

(3) strategic leaders who feel risk is intrinsic in their decisions and ERM would be redundant in this context.

Those setting strategic direction may not have the luxury or desire to spend much time on what might be called risk analysis. To help address point 1, it is crucial to make use of tools that may be employed with minimal time investment yet clear, tangible benefit. One such concept is a rating of a strategy's alignment with delineated risk appetite. It measures (numerically or qualitatively) the amount and types of risk that a proposed strategy would create for the company and compares those to the organization's risk appetite and defined limits. The concept is simply to determine whether the expected exposures are in line with tolerances and preferences for risk amount and type.

The challenges identified in points 2 and 3 can largely be addressed by using the LFA-based approach to strategic risk assessment and stressing subgoal attainment as the foundation of the process, rather than beginning by asking for a "top risk list." In addition, by quantifying and prioritizing risks using metrics inherent in business line and management decisions, the risk manager can produce intelligence that resonates with key decision makers.

Portfolio View

From ERM's humble beginnings, the portfolio or holistic view of risk has been consistently stressed. Because an organization can be well managed only when its risk-reward profile is understood in an accurate and comprehensive manner, the portfolio view is almost universally regarded by practitioners as a critical ERM outcome.

This objective is at risk due to several factors, including (1) failure to include all relevant risk sources, (2) the inability to aggregate risk properly and (3) a lack of metrics that highlight critical exposures.

We have discussed the importance of capturing all functional areas, locations and departments in the risk assessment process. By ensuring a wide "risk net" and also carefully tracking potentially unseen exposures such as third-party risks, reputational effects and emerging risks, risk factor number one can be avoided.

To address the second factor, it is important to have a clear understanding of correlation and interrelationships across risk types and events. Although not necessary to employ a "full-blown" stochastic model that must be run overnight, it is important to make use of mathematical and statistical notions that capture the practical effects of "intertwined" risks. At the very least, "do no harm" with faulty mathematics.

To ensure that all critical exposures are captured, the ERM framework must employ a suite of metrics that capture all relevant quantities. This means that at insurance companies, one needs some metric relating to capital requirements and usage, and at U.S. public companies we must include GAAP earnings severity estimates in our arsenal. Additionally, because some risks unfold over a number of years, or have an effect only over long time horizons, the framework must have long-term value metrics such as a present value of free cash flows or a risk-intelligent business valuation.

PARTING THOUGHTS

It (almost) goes without saying that risk environments evolve, organizations change over time and available data and computing methods continue to expand. By incorporating the Guidance's suggestions for self-learning, review and revision, and targeted use of technology, a company that has attained an advanced ERM maturity can help ensure it continues to stay that way. ■

Damon Levine, ARM, CFA, CRCMP, is senior vice president, Enterprise Risk, at the Beneficient Company Group. He can be reached at *damon.levine@beneficient.com*.

ENDNOTES

1 COSO. *Enterprise Risk Management Integrating with Strategy and Performance (Executive Summary)*, June 2017, *https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf* (accessed April 22, 2019).

2 See, for example, Leonellha Barreto Dillon, Logical Framework Approach, *Sustainable Sanitation and Water Management*, April 27, 2018, *https://sswm.info/planning-and-programming/decision-making/planning-community/logical-framework-approach.*