



IT MIGHT BE A GOOD TIME TO ‘DUST OFF’ THAT ERM DOCUMENTATION

Spring cleaning! Granted, it does not generally make the list of the top five things most people enjoy about this time of year, but it does serve a purpose. And we do enjoy the benefits that result from a little elbow grease and a little polish! This spring particularly might be a good time to pull out your organization’s ERM documentation and spiff it up.

First, let’s start by assuming your organization has an ERM. If you are asking yourself, what is an ERM, that’s not a good sign. Enterprise Risk Management is a methods-based process of determining and managing business risk.

ERM really came into its own with the enactment of the Sarbanes-Oxley Act (SOX) in 2002 requiring that public companies maintain and certify that a system of internal controls was in place and

functioning to accurately manage and report key business processes. This was followed in 2004 with the COSO Enterprise Risk Management – Integrated Framework that outlined a structure for identifying key areas of risk, identifying an organization’s appetite for these risks and assigning responsibility for managing risk within the framework.

The ERM has served as a foundational step to developing the internal control systems that satisfied the requirements of SOX.

The COSO framework requires that an organization systematically identify and prioritize risks. Once risks are identified, they must be assessed in a four-step process:

- 1) Develop assessment criteria – this involves determining a ranking scale, which generally ranks individual risks

by magnitude of impact and likelihood of occurrence.

- 2) Assess risks – risks are qualitatively identified and then the more important or material risks are quantified based on the step 1 criteria.
- 3) Assess risk interactions – the relationship of individual risks is determined, which may entail a re-ranking of these risks after step 2.
- 4) Risks are then prioritized based on their potential impact on the goals of the organization.

The ERM is intended to be a living process, regularly revised and updated to reflect the evolving nature of the business and the environment in which it operates. Unfortunately, many organizations shelved the exercise once the internal control framework was established and only pay it lip

service when the topic of risk comes around on the board agenda.

This spring offers a unique opportunity to revisit the ERM and test some of the assumptions and judgments that are implicit in the process. The past few years (2018 – 2021) have seen several major occurrences that individually and in combination pressure test an enterprise's assumptions with regard to identified risks and the effectiveness of its risk mitigation strategies.

The tariffs imposed by President Donald Trump in 2018 as part of the effort to renegotiate the North American Free Trade Agreement quickly escalated and ultimately focused on trade with China. Cybersecurity lapses tested the integrity of technology, particularly within our financial systems. Then COVID-19 forced closure of large sections of the economy and stressed both supply chains and distribution channels as businesses were forced to make difficult decisions to maintain liquidity. Social unrest stemming from police actions in Minnesota and Georgia added further tensions to the marketplace.

These events occurring in rapid succession created a unique environment in which to review the ERM, as well as risk management strategies that evolve from it.

The COSO framework delineates four objective categories within which to classify organizational risk. Working within that framework, it might be beneficial to explore how this sequence of recent events could alter the evaluation of risk and how it is managed.

Strategy

The first objective category entails the high-level goals of the organization and their alignment

with the overall mission statement. These are risks at the highest level and involve strategy rather than tactics. For example, is the organization positioning itself as a cash yield investment or as a growth company? Are acquisitions an important component of the company's strategy? Is vertical integration desirable?

With these goals in mind, those responsible for maintaining the ERM should consider how recent events have affected the organization's reputation in the marketplace. The tariff wars have radically altered cross border relationships while the focus on social justice has brought an intense spotlight on the practices of many organizations. This should cause a review of potential merger candidates, major suppliers and service providers, and the organization's advertising and marketing strategies.

This spring particularly might be a good time to pull out your organization's ERM documentation and spiff it up.

Operations

A major focus of internal controls is the effective and efficient use of the enterprise's resources. The disruption of the market caused by the trade disputes and COVID-19 are a good testing ground for any organization's risk assumptions regarding its supply chain and distribution channels. The disruptions in the spring of 2020 in staple food items and hard goods highlighted just how vulnerable operations can be.

The organization's workforce is an area that should not be overlooked. As many companies were forced to furlough workers last year, this would be a good time to assess how staff responded and the degree to which such extreme measures put the operations at risk.

Financial Reporting

The requirement of shelter in place for several months tested contingency planning for financial reporting and stressed compliance within the control environment. This coupled with the increased risk of cybersecurity breakdowns should cause organizations to review how these risks are managed. It could also change whether processes are managed in-house or outsourced as the organization determines its appetite for risk and how to most effectively mitigate it.

Compliance

Finally, as organizations were required to react to rapidly changing conditions, compliance with applicable laws and regulations can often be compromised. In addition, weaknesses in the compliance structure may be revealed. This may call for a review of standard contracts and terms with both suppliers and customers. For example, do contracts have adequate provision for force majeure and have claims arisen that were not foreseen prior to recent past events?

In summary, before the confluence of these major events fade, management owes it to the organization, its investors, creditors and other constituents to take a fresh look at its appetite for business risk and how it manages the risk.

ABOUT THE AUTHOR: Don Carpenter is clinical professor of accounting at Baylor University. Contact him at Don_Carpenter@baylor.edu.