 ISBN : 9780974211428

Moving From Enterprise Risk Management to Strategic Risk Management: Examining the Revised COSO ERM Framework

Elizabeth M Pierce
Saginaw Valley State University
University Center, MI

James Goldstein
Canisius College
Buffalo, New York

Corresponding Author:
Elizabeth Pierce
Assistant Professor of Accounting
Saginaw Valley State University
7400 Bay Road, Curtiss 307
University Center, MI 48710
(989) 964-4017
empierce@svsu.edu

Professional Biographies:

Elizabeth Pierce is an assistant professor of accounting at Saginaw Valley State University. A former CPA, Dr. Pierce holds a Ph.D. in immunology from University of Michigan-Ann Arbor. To qualify to teach accounting, she completed the AACSB's Postdoctoral Bridge Program in Accounting and Finance. Her teaching interests include managerial and cost accounting, as well as accounting information systems. Her research interests include Enterprise Risk Management, cyberbreach and continuous montoring/auditing.

James Goldstein is an associate professor of accounting at Canisius College in Buffalo, New York. James is a CPA and holds a Ph.D. in Management Information Systems from Syracuse University and an MBA in Finance and Economics from the Stern School of Business at New York University. Prior to academia, he worked in public accounting, at a Wall Street investment bank, and at a regional bank in upstate New York. His teaching interests include financial accounting and accounting information systems. His research interests include Enterprise Risk Management, the Balanced Scorecard, and Accounting Information Systems.

 ISBN : 9780974211428

Moving From Enterprise Risk Management to Strategic Risk Management: Examining the Revised COSO ERM Framework

Purpose:
The purpose of this paper is two-fold: (1) to examine the initial COSO ERM Framework (2004) with the purpose of determining the shortcomings that may have led to a siloed view of strategy setting and ERM, and (2) to examine the proposed Framework (2016) with the purpose of determining whether the identified shortcomings are effectively addressed.

Design/methodology/approach:
This study will compare the original guidelines with the current published evaluation draft of the revision. Analysis of published surveys will help pinpoint the issues that were hopefully addressed in the revisions.

Findings:
Strategic and organization risks had been siloed by many corporations following the original 2004 ERM guidelines. In the evaluation draft, it is clear that COSO made an attempt to bring these two aspects together for a more solid, effective ERM.

Research limitations/implications:
The current draft is an evaluation draft published with the intent of getting feedback on the changes. The deadline for public feedback is shortly after this meeting. Any changes will not be available for a time after this paper is completed.

Practical implications:
The purpose of the ERM guidelines is to give risk managers and internal auditors guidelines for strategic planning for risk. This analysis will provide insight to these individuals into the changes in the new guidelines that will allow for more efficient and effective strategic planning.

Originality/value:
Since the evaluation draft was issued in June, there is no published analysis of the new proposed guidelines. Thus, this represents and original publication.

Keywords: Enterprise Risk Management, COSO, Strategic Planning, risk appetite

 ISBN : 9780974211428

Moving from Enterprise Risk Management to Strategic Risk Management: Examining the Revised COSO ERM Framework

Introduction

In 2004, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published the *Enterprise Risk Management – Integrated Framework.* The Framework has since become recognized as a best practice guidance concerning the management of risk in organizations throughout various industries within the United States. However, despite the Framework's widespread acceptance, a survey by COSO in 2010 found that the state of enterprise risk management (ERM) was relatively immature for a majority of the respondents. In particular, the survey found that many of the respondents neglected to consider their organization objectives in the context of their desired risk appetite. One potential explanation for this practice is the perspective that ERM is simply another compliance function, as opposed to providing insight into the setting and achievement of strategic objectives.

A survey conducted by the Financial Executives Research Foundation (Metha, 2010) during the same period came to similar conclusions. The FERF survey indicated that responding organizations had a siloed view of risk, either focusing on strategic or operational risks, at the expense of the other. Both the COSO and FERF surveys appeared to show that companies were conducting strategic planning and risk management as separate practices, thereby significantly limiting the benefits of ERM.

In June 2016, COSO released an exposure draft of an update to the 2004 Framework for public comment. *Enterprise Risk Management – Aligning Risk with Strategy and Performance* is more explicit in stressing the need to consider business objectives in the context of risk appetite. The purpose of this paper is twofold: (1) to examine the initial COSO ERM Framework (COSO 2004) with the purpose of determining shortcomings that may have led to a siloed view of strategy setting and ERM, and (2) to examine the proposed Framework (2016) with the purpose of determining whether the identified shortcomings are effectively addressed in the revised document.

A History of COSO

COSO is a voluntary private sector initiative dedicated to improving organizational performance and governance through effective internal control, enterprise risk management and fraud deterrence. Five nonprofits are its sponsoring organizations: American Accounting Association (AAA), American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), Institute of Internal Auditors (IIA) and Institute of Managerial Accountants (IMA) (McNally, 2013).

Organized in 1985, COSO was meant to sponsor the National Commission on Fraudulent Financial Reporting. The focus of this independent private-sector initiative was to study the casual factors that can lead to fraudulent financial reporting. Since being founded, it has also developed recommendations for public companies and their independent auditors, for the U.S. Securities and Exchange Commission (SEC) and other regulators, and for educational

institutions (COSO, 2016). As mentioned above, the National Commission was sponsored by five major professional associations. The Commission, which is wholly independent of all sponsoring organizations included members from public accounting, investment firms, industry and the New York Stock exchange. The current chairman of COSO is Robert B. Hirth, Jr. (COSO, 2016).

COSO's goals have evolved to include ERM, internal control and fraud deterence. In 2004, COSO issued *Enterprise Risk Management – Integrated Framework.* Since that time, they have also published several thought papers to deal with specific questions and issues with implementation of the ERM guidelines. COSO is highly regarded as the authority for internal control guidance, and because of this, it seemed logical for them to expand into ERM.

The Original Guidelines

Included in the ERM guidelines is the COSO ERM Cube (see Fig 1). The cube defines the components, objectives and categories of ERM management. Most important, it seemed was the categories which included: Strategic, Operations, Reporting and Compliance. The cube would provide a framework for undertaking ERM. The cube links the ERM to Sarbanes-Oxley requirements for companies listed on United States stock exchanges (AIRMIC, Alarm, & IRM, 2010). Since risk management focuses on the identification of threats and opportunities, with controls designed to effectively counter threats and take advantage of opportunities, risk management can be considered one side of the coin with internal control being the other (McNally & Tophoff, 2014). COSO's *Internal Control – Integrated Framework* was issued in 1995 to help businesses and other entities asses and enhance their internal control systems. The internal control guidelines have been incorporated into policy, rules and regulations used by thousands of enterprises to better control their activities. These guidelines have become even more important since the created of the SOX Act (COSO, 2013).

One of the goals of the original guidelines was the incorporation of risk management to strategic planning. The guidelines were intended to help risk managers identify potential risk events that may affect the entity and manage risk to be within its risk appetite, to provide reasonable assurance in achievement of the entity's objectives (COSO, 2004). The frame work deals with risk avoidance, acceptance, sharing and reduction (D'Aquila & Houmes, 2014). The 2004 ERM guidelines were a first attempt to recognize the interdependencies among risks and then treatment of risks across all business operations (Dafikpake, 2011).

In 2008, there were indications that companies were frustrated with attempts at implementing the ERM framework. Purdy identified that companies were dissatisfied with the progress made in implementation and were seeking an approach more relevant to strategic management of their business (2008). In 2009, COSO issued a thought paper, *Effective Enterprise Risk Oversight: The Role of the Board of Directs.* In this paper, COSO suggested that the main challenge facing boards of directors is finding effective manner to oversee managing risk while bringing value to the company (COSO, 2004). Several surveys were implemented to get a better gauge on the implementation issues that companies faced.

The Surveys

On December 9, 2010, COSO released two thought papers based on surveys on the current state of ERM and Board Risk Oversight. In the 2010 Report on ERM, Beasley, et. al., found that of 460 respondents, 60% admitted that they had informal and ad hoc risk management processes with almost half describing their organization's understanding of ERM processes as "very immature" or "somewhat immature". Almost one-third admitted that they were either "not at all" or "minimally" satisfied with the report of key risk indicators to senior executives. Yet, overwhelmingly, companies surveyed chose the COSO framework as a basis of implementation, despite the availability of other frameworks (Beasley, et. al., 2010). In the Board Risk Oversight paper, Protiviti surveyed 200 corporate directors about their knowledge of the Framework and the current state and desired state of the process as applied by their board of directors. Despite a high rate (53%) of directors who believed their process was "effective" or "highly effective," most (70%) felt the oversight process executed by their boards was immature (Protiviti, 2010).

To add to these results, the Financial Executives Research Foundation (FERF) issued a report on a similar study. FERF reviewed ERM programs at more than 40 companies and interviewed 25 mainly Fortune 500 companies. When asked about the current state of ERM implementation, these organizations generally believed that the ERM process exists to make risks more visible before they can have an impact. However, overall, the ERM programs at these organizations were again, found to be immature, in the early stages of implementation (Mehta, 2010. A third survey was conducted by the IIA asking 47 questions relating to the use and implementation of both COSO frameworks (PWC, 2015). ……(results of survey if useable).

These results of these surveys as well as the quickly changing risk in business created a need for update of the framework. Thus, in February, 2015, COSO embarked on a revision of the framework. During this timeframe, The International Organization on Standards (ISO), who provided the other major framework on ERM, called ISO31000, began a revision of their guidelines as well.

The Revisions

On June 14, 2016, COSO released their exposure draft, "Enterprise Risk Management – Aligning Risk with Strategy and Performance." The first noticeable difference with the framework was an emphasis aligning risk with strategic and operational planning. While strategy and operations were two of the categories included in the first guidelines, there was little understanding of how these things were interrelated. Clearly, there was a silo effect that COSO wanted to eliminate in this version of the guidelines. To that effect, the second noticeable difference was the removal of the ERM cube. In its place was a new model (Fig 2) that showed ERM as a cycle with an arrow through it all indicating that every leads to the next step. Now there is an emphasis on alignment with the company's mission, vision, and core values (COSO, 2016). Further, the language of the new framework is explicit about the need to apply risk appetite to strategic and business process planning. Only then will a company see continued enhanced performance.

In answer to the comments that the framework is immature in how to apply the risk appetite, COSO has provided tools to help companies envision where their planning aligns to the company's risk appetite and risk capacity. The graphs (Fig 3) are intended to give companies a visual record of where these three things stand in relationship to each other (COSO, 2016).

Conclusion

There are clear changes to this framework with the exposure draft. The revisions were born out of a need to provide more mature guidance for application of risk management to strategic and operational planning. The concept of risk appetite, new in the 2004 framework, was confusing to risk managers and the original framework did not provide clear guidance of how to gauge risk appetite or how it could enhance performance when used as a guide to the amount risk taken in these plans. It was believed that the Cube being present in both the Internal Control framework and the 2004 ERM framework encouraged enterprise risk managers to try to apply the guidelines in conjunction with each other. Further, the Cube did not represent the cyclical nature of ERM planning and the separation of the categories may have caused the silo effect of doing planning separately for strategic and operational goals

The new guidelines, clearly, have the intent of providing more guidance for the application of risk appetite to both strategic and operational planning. They also encourage the view that all risk planning decisions should be aligned with the mission, vision, and core values of the firm. Further, the new diagram encourages a cyclical process for ERM planning that applies to both strategic and business process planning. By keeping these things in mind in the planning process, ERM should enhance the performance of the firm.

Because the framework is in comment period, COSO has released several of the comments on their website. A quick assessment of the comments produces the following: Several of the commenters believe that COSO has not gone far enough in their guidance. Rather than a framework, they would like better definitions, rules for applying/assessing/setting risk appetite, as well as how the management and board should oversee (Maciel, 2016; Leigh, 2016; Marks, 2016; van de Ven, 2016; Seetho, 2016;). There is a recurring theme that the elevation of strategy as a goal is misplaced and that the definitions of strategic risk is unclear or even confused with management strategy (Doney, 2016; Finn, 2016; Mellendijk, 2016; Leigh, 2016; van de Ven, 2016). Some even suggest that rather than moving away from the Internal Control framework, they should move closer (Finn, 2016; Leigh, 2016; Leech, 2016). Further, a couple suggest that definitions might have been left out of this exposure draft because they are explained in the Internal Control Framework and COSO may be trying to reduce redundancy between the two frameworks. However, given that they seem to want to establish ERM as a separate function, this makes the framework hard to understand (Gwin, 2016; Leigh, 2016; Marks, 2016). Finally, there are several of the commenters who just did not like the new diagrams and tools given in the new draft. They feel they are hard to understand (Doney, 2016; Maciel, 2016; Marks, 2016; Seetho, 2016; Ayse & Nordal, 2016).

Clearly there is still more work to be done. While many of these commenters want more specific guidance, it is easy to understand why COSO did not go that far. As with most guidelines, COSO may want to just provide food for thought, while the expectation would be

that individual companies would their own risk management principles to meet their unique needs. A framework that give too much specific guidance would be difficult to adapt to all cultures.

While this exposure draft is the latest version of this framework, it is in a comment period that ends on September 30, 2016. From that point, the committees will review the comments and make any necessary revisions. Hopefully, the revisions will be small and they will quickly release the final version of the draft. At that time, it would be good to update this report with any changes that are made to the framework.

 ISBN : 9780974211428

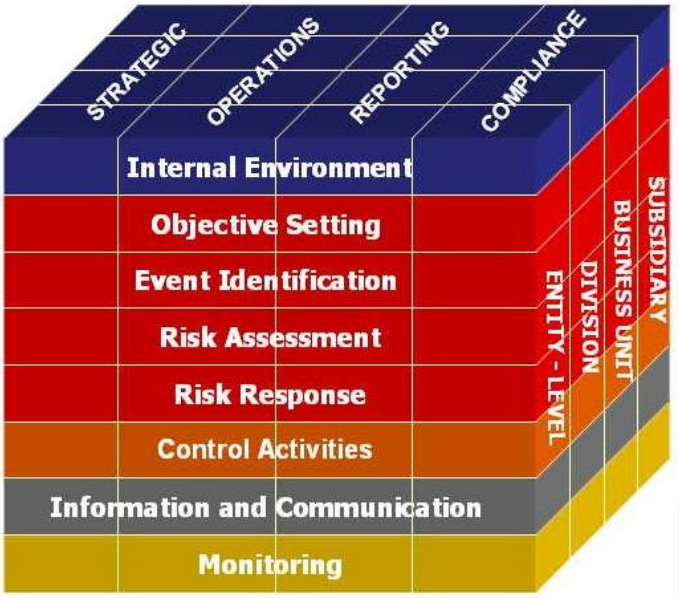

Figure 1: 2004 COSO ERM Cube: This cube represents the Components, Objectives, and Categories of effective ERM planning. The top represents the categories of ERM planning, the front represents the objectives and the right side represents the components of the business. Together the cube represents the process of ERM planning (COSO, 2004).

 ISBN : 9780974211428

Figure 2: 2016 COSO ERM components: The new diagram indicates that all risk decisions should be aligned with the company's mission, vision and core values. The components for risk decisions are applied to strategy and business objectives resulting in enhanced performance.

 ISBN : 9780974211428

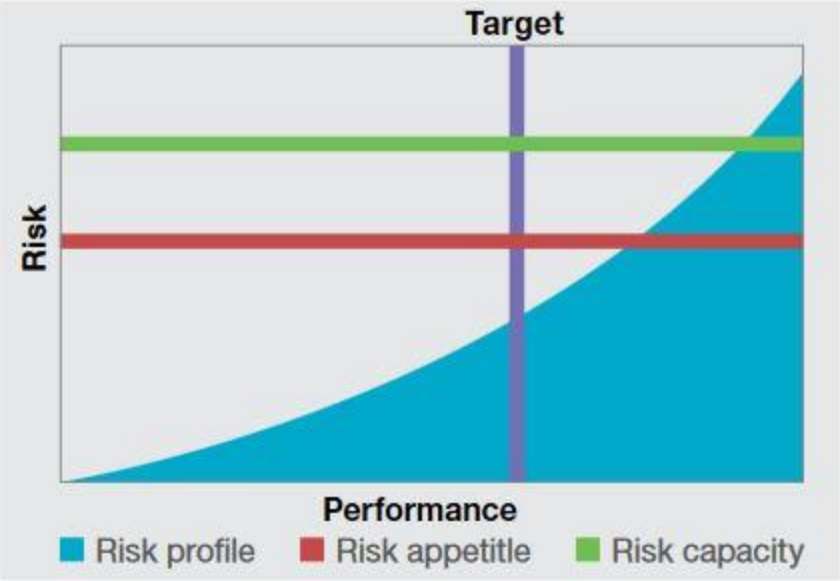

Figure 3: Risk profile showing risk appetite and risk capacity. The graph attempts to give companies a visual way to gauge whether they are taking advantage of their risk appetite in their strategic planning. The purple line shows the target risk based on risk appetite while the blue curve indicates the current risk profile of the company's planning. According to this graph, this company could absorb more risk which would allow them to enhance their performance even more.

Bibliography

The Association of Insurance and Risk Managers, Alarm, and The Institute of Risk Management. (2010) "Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000", available at: http://competency.aicpa.org/media_resources/206771-a-structured-approach-to-enterprise-risk-management/detail (accessed 20 March, 2016).

Ayse, Y. & Nordal, B. (2016), "Feedback to Document <Enterprise Risk Management, Aligning Risk with Strategy and Performance", available at http://erm.coso.org/Pages/Viewcomments.aspx. (accessed 22, September, 2016).

Beasley, M.S., Branson, B.C., and Hancock, B.V. (2010), "COSO's 2010 Report on ERM: Current State of Enterprise Risk Oversight and Market Perceptions of COSO's ERM Framework", available at: http://coso.org/-ERM.htm. (accessed 17 September, 2016).

Committee of Sponsoring Organizations of the Treadway Commission. (2004), "Enterprise Risk Management – Integrated Framework", available at http://coso.org/-ERM.htm. (accessed 18 May, 2016).

Committee of Sponsoring Organization of the Treadway Commission (2016), "Enterprise Risk Management: Aligning Risk with Strategy and Performance", available at: http://erm.coso.org/Pages/viewexposuredraft.aspx. (accessed 20 June, 2016).

D;Aquila, JM, and Houmes. R. (2014) "COSO's updated internal control and enterprise risk management frameworks", The CPA Journal: pp 54-59.

Doney, D. (2016) "Comments on COSO ERM Framework Draft", available at http://erm.coso.org/Pages/Viewcomments.aspx. (accessed 22, September, 2016).

Finn, JJ. (2016), "Critique and Comments on COSO ERM update", available at http://erm.coso.org/Pages/Viewcomments.aspx. (accessed 22, September, 2016).

Gwin, J. (2016), "Comments on the COSO ERM Exposure Draft", available at http://erm.coso.org/Pages/Viewcomments.aspx. (accessed 22, September, 2016).

Leech, T. (2016), "Comments on the June 2016 COSO draft "Enterprise Risk Management: Aligning Risk with Strategy and Performance"", available at http://erm.coso.org/Pages/Viewcomments.aspx. (accessed 22, September, 2016).

Leigh, N. (2016), "Impressions of The COSO ERM Public Exposure 2016", available at http://erm.coso.org/Pages/Viewcomments.aspx. (accessed 22, September, 2016).

Maciel, D.S. (2016), "Enterprise Risk Management: Aligning Risk with Strategy and Performance" [comments], available at http://erm.coso.org/Pages/Viewcomments.aspx. (accessed 22, September, 2016).

Marks, N. (2016), "Reflections and feedback on the COSO ERM 2016 Update:", available at http://erm.coso.org/Pages/Viewcomments.aspx. (accessed 22, September, 2016).

Mellendijk, JP. (2016) Enterprise Risk Management: Aligning Risk with Strategy and Performance" [comments], available at http://erm.coso.org/Pages/Viewcomments.aspx. (accessed 22, September, 2016).

McNally, J.S. (2013) "The 2013 COSO Framework & SOX Compliance: One approach to an effective transition", Strategic Finance: pp 45-52.

McNally, J.S. and Tophoff, V.H. (2014) "Leveraging Effective Risk Management and Internal Control", Strategic Finance: pp 29-36.

Metha, S. (2010), "Enterprise Risk Management Insights & Operationalization" [Executive Report], Danvers, MA: Financial Executives Research Foundation.

Protiviti (2010), "Board Risk Oversight – A Progress Report: Where Boards of Directors Currently Stand in Executing their Risk Oversight Responsibilities", available at: http://coso.org/-ERM.htm. (accessed 17 September, 2016).

PWC (2015), Survey Findings for the COSO Advisory Council Meeting on February 3, 2015. Not Published.

Purdy, G. (2008) "How to Bring Your ERM Framework Into Line With ISO31000", in Lexis Nexis 5th Annual Risk Management Conference Sydney, Austrailia, 2008, available at: http://www.lexisnexis.com.au/Risk2008: pg 26.

Seetho, S. (2016), Feedback on the COSO ERM 2016 Public Exposure Draft from Singapore", available at http://erm.coso.org/Pages/Viewcomments.aspx. (accessed 22, September, 2016).

van de Ven, A. (2016), "Comments on the public Exposure Draft COSO – Enterprise Risk Management framework", available at http://erm.coso.org/Pages/Viewcomments.aspx. (accessed 22, September, 2016).