The ERM Framework

1

Learning Objectives

After completing this reading, you should be able to

- Explain the rationale for developing and describe the elements of an ERM framework
- Describe recommended practices for the development and governance of an ERM framework

Excerpt is Chapter 7 of Implementing Enterprise Risk Management – From Methods to Applications*, by James Lam.*

CHAPTER 7

The ERM Framework

INTRODUCTION

In managing something as complex as a large corporation, or even a single function within such an organization (including ERM), it's easy to miss the forest for the trees. That is, one can quickly lose track of the big picture by getting caught up in the details. At the other end of the spectrum, too broad a view can lead one to overlook something important. In order to establish a structured approach, businesses have been implementing management frameworks that encapsulate the big ideas of a complex topic while breaking them down into discrete components. Early frameworks, such as the BCG Matrix (1968) and Porter's Five Forces (1979), focused on competitive analysis and strategy formation. Others, notably the Balanced Scorecard developed in 1987, focused on performance management and reporting. However, none of these frameworks directly address risk.

In this chapter, we'll begin by examining the nature and usage of frameworks in general. We'll next consider why organizations need a workable ERM framework that can coexist alongside (or within) these broader frameworks. Then we'll establish criteria to evaluate the usefulness of an ERM framework. I'll also offer my own take on an ERM framework that I think many companies can adapt for their own use.

THE NEED FOR AN ERM FRAMEWORK

I hope the previous chapters have made it clear why ERM is so important in today's business climate, but why do we need an ERM framework? Why can't current management structures simply incorporate risk management? Big companies have been functioning for a long time without ERM models, so it's a fair question.

The first part of the answer is that a framework is a communication tool. We use frameworks to transmit ideas in other areas of the business world; it

only makes sense to use one for something as complex as ERM—especially since it remains a poorly understood topic outside the practice of risk management itself. Effective ERM requires a great deal of coordination and collaboration horizontally—among departments—and vertically, within organizational units. A simple framework helps each cohort visualize its role. For example, the three lines of defense against risk—business units, corporate management, and the board—are most effective when each understands the entire defensive structure. (We'll examine the lines of defense in complete detail in the next chapter.) An ERM framework also aids communication within a business over time, irrespective of executive turnover. It establishes a consistent basis for evaluating the company's risk management efforts and those of other companies in order to establish industry standards.

Frameworks help manage complexity as well. The number of risks that face organizations is ever-growing: strategic, financial, operational, reputational, legal- and compliance-related, and more recently, cybersecurity. These manifold challenges are interconnected, often in subtle ways that require careful analysis. Organizational complexity also factors into the equation, including meeting the needs of multiple business units and control functions, internal audit, and external regulators. In addition, an organization must have multiple lines of defense that interact dynamically even as they respond to risk events in real time. With this Byzantine level of complexity—not to mention the high stakes involved—organizations need a guiding framework to ensure that no one is duplicating effort and nothing slips through the cracks.

Strategic Frameworks

When designing a framework for ERM, it is helpful to look at management frameworks that have endured over time to determine the qualities that made them successful. Here are four strategic frameworks—three familiar, one quite new—that can serve as benchmarks for our own efforts.

BCG Matrix Figure 7.1 shows the BCG Matrix. This simple four-part matrix, created in 1968 by the Boston Consulting Group, illustrates the value potential of different business units across market growth (which consumes cash) and market share (which generates cash).[1] A star business unit is one that experiences both high growth and high market share. Cash cows are those that require little cash input yet hold onto market share nonetheless. By categorizing business initiatives in this way, a company can determine where to invest for the future. Note that the matrix does not offer a solution, but simply a clearer depiction of the issue at hand.

Porter Five Forces Figure 7.2 shows the Porter Five Forces model. Michael Porter of Harvard University devised this framework in 1979 to represent

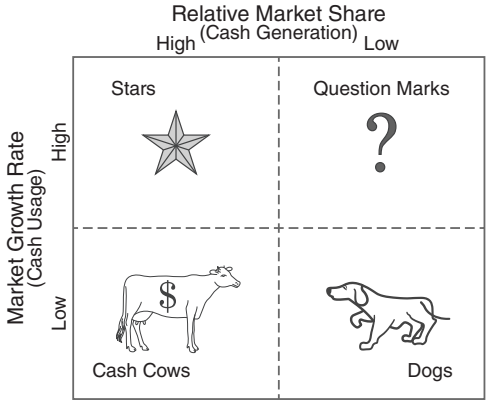

FIGURE 7.1 BCG Matrix
Bruce Henderson, "*The Product Portfolio*."
Retrieved December 26, 2016

FIGURE 7.2 Porter's Five Forces
Michael E. Porter, "The Five Competitive Forces that Shape Strategy," *Harvard Business Review*, January 2008, p. 86–104

the competitive threats to a company within its industry.[2] Porter saw this framework as a more rigorous alternative to SWOT (strengths, weaknesses, opportunities, treats) analysis. Each of these forces affects a company's ability to serve its customers and make a profit. Two competitive threats (substitute products or services and new entrants) and two supply-chain forces (the bargaining powers of suppliers and customers, respectively) exert continual pressure, while a third competitive threat, established rivals, is both central and cyclical.

The Balanced Scorecard The Balanced Scorecard (Figure 7.3) was introduced by Bob Kaplan and David Norton in 1992 as a technique for evaluating management performance based on the organization's vision and strategy.[3] Its greatest innovation is including non-financial elements alongside financial ones, which makes it perennially relevant to today's holistic view of business leadership. At its heart is the vision and strategy

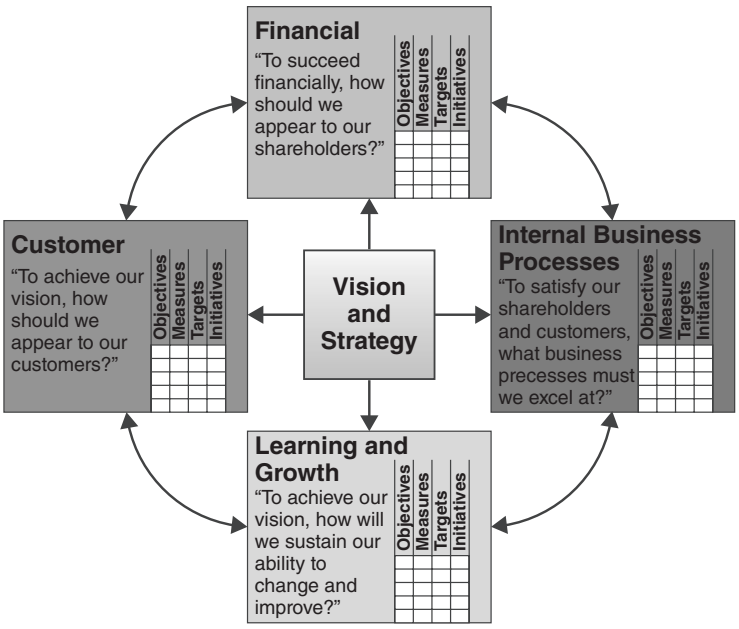

FIGURE 7.3 The Balanced Scorecard
Kaplan, Robert S., and Norton, D. P. (1992). "The Balanced Scorecard—Measures That Drive Performance," *Harvard Business Review* (January–February): 71–79

	Disruptive Innovation	Sustaining Innovation
Revenue Performance	Transformation Zone: Horizon 2	Performance Zone: Horizon 1
Enabling Investments	Incubation Zone: Horizon 3	Productivity Zone: Horizon 1

FIGURE 7.4 Moore's Four Zones
Geoffrey A. Moore, "Zone to Win," Diversion Books, November 3, 2015

of the organization, which inform the other elements of the framework: financial, customer, internal processes, and learning and growth. The Balanced Scorecard is valuable also for its structure, which emphasizes feedback loops in which measured results spur continuous improvement.

Moore's Four Zones In his 2015 book, *Zone to Win*, Geoffrey Moore sets out a framework to help mature companies with a growing problem: defending themselves against paradigm-shifting technology that disrupts their incumbent franchises.[4] The framework (Figure 7.4) follows a portfolio model, allocating strategic resources along three investment horizons: Horizon 1 is the coming fiscal year; horizon 2, one to three years; and horizon 3, three to five years. Established franchises live on the sustaining side of this matrix and focus on the shortest horizon. Emerging businesses gestate in Horizon 3 as they might in a venture capital portfolio: Weaker ones fail quickly and inexpensively while stronger bets win additional resources. When an investment in that stage shows enough promise to bring to scale, it can move into Horizon 2 supported by greater investment to propel it into a revenue-producing business.

ERM FRAMEWORK CRITERIA

As you can see, one obvious problem with these frameworks is that they do not explicitly address risk. For that reason, there have been several attempts over the past few years to create a workable risk management framework. In doing so, however, we must not forget the lessons these enduring models offer. Like them, an ERM framework must be simple, comprehensive but

not repetitious, balanced and integrated, flexible, and, of course, effective. Here's a closer look at each of these criteria:

Simple: When it comes to guiding principles, simplicity is key. Simple ideas can be communicated clearly and applied with accuracy. If a framework is overly complicated, it will be difficult to communicate, to implement, and to evaluate. Take the example of a roadmap. Drivers need enough detail to get their bearings and determine which turns to take. But if a map is cluttered with unnecessary information such as terrain and other details, it will be difficult to follow. Likewise, a strong ERM framework should provide enough structure to guide highly detailed decisions, but not be so comprehensive as to cloud the decision-making process. I believe a good rule of thumb for any framework is 5 +/– 2 (i.e., 3–7) components because research studies have shown that is the sweet spot for human memory.

Mutually Exclusive, Collectively Exhaustive (MECE): This attribute is composed of two parts that complement one another. First of all, the components of a good ERM framework are *mutually exclusive*, meaning that each is unique with no overlap. Second, the framework should be *collectively exhaustive*. It should be comprehensive enough to apply to every part of the organization and account for every eventuality. Returning to the roadmap example: A map should be exhaustive enough to be useful for any driver, whether a tourist, a road-tripper, or a businessperson. Creating separate maps for each driver's purpose would be inefficient, as it would generate a great deal of duplicate information. A strong ERM framework should be informative and applicable to every level of management without containing redundancies.

Balanced and Integrated: An ERM framework shouldn't overemphasize any aspect of risk management at the expense of others. An unbalanced framework could lead to a breakdown in communication or inadequate preparation for a certain type of risk. In addition, it must be integrated into the context of the organization. A framework may be flawless in theory, but if it clashes with the well-oiled operations of the existing management structure, it simply won't work. Each element of the model complements the others while also supporting the organization as a whole. A strong framework should resemble an auto engine, with each piece fitted precisely with the next to work in harmony, while also working with other components (steering wheel, accelerator) that the vehicle relies upon.

Flexible: Risk is by its nature unpredictable. Industry dynamics, business models, and disruptive technologies are constantly changing. Just as ERM processes must protect against unforeseen risk, so too must the framework encompass the unknowable while still embracing the organization's long-term vision. A strong ERM model will be broad and inclusive enough to remain relevant through changes in business plans and market conditions. While particular ERM strategies and defensive plans will evolve as an organization does, the framework should be a flexible template to guide that evolution.

Effective: Of course, we all care about the bottom line. An ERM framework isn't any good if it doesn't actually prepare an organization for negative events or bring opportunities to light. The effectiveness of a framework reflects its impact within the organization. This criterion should be applied judiciously, however, as the effectiveness of a framework relies heavily on how well it is implemented (which has its own challenges for evaluation). The effectiveness of an ERM framework can be measured by the extent it is integrated into business and risk decisions, as well as its contribution to producing the desired business outcomes.

CURRENT ERM FRAMEWORKS

While I believe that each organization should customize its own ERM framework, there's certainly no reason to reinvent the wheel every time. For that reason, a broadly accepted, standardized model is a worthy goal. Two such models are in use today internationally and across industries: the COSO ERM framework, and the Australia/New Zealand framework (AS-NZS), also known as ISO 31000. The two frameworks take very different approaches to risk management and are suited to different kinds of organizations. The COSO framework, frequently used by large corporations, is highly structured and detailed. ISO 31000 is less prescriptive and more process based.

The COSO Framework

The most widely used ERM framework globally comes from the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Formed in the mid-1980s to help companies comply with new federal anti-fraud legislation, COSO is a joint initiative of five major U.S. accounting industry organizations, including the Institute of Management Accountants (IMA),

the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), the Institute of Internal Auditors (IIA), and Financial Executives International (FEI). In cooperation with PricewaterhouseCoopers, COSO published a framework for internal control in 1992, which it adapted in 2004 as an integrated ERM framework. The COSO framework was meant to be robust in its approach to risk and readily usable by management teams as they identify, assess, and manage risk.[5] The main distinguishing quality of this framework is its thorough inclusion of all possible risk levels and responses. In fact, it is so extensive that its complexity can work against it, making it unwieldy for some businesses.

In the spirit of full disclosure, I have been a vocal critic of the COSO 2004 ERM framework, both as a conceptual framework and as it is applied in ERM programs. My major conceptual criticisms centered on its complexity and that some of the components are not MECE (two of the key criteria discussed above). My major practical criticisms involve its application in risk assessments and the use of probability and severity ratings in prioritizing risks. Moreover, I do not believe the framework adequately addresses risk/return tradeoffs and the management of unexpected variance in business performance. However, I do believe the framework has contributed net benefits in ERM with respect to promoting awareness of ERM at the management and board levels as well as linking ERM to entity objectives.

Despite my known criticisms of the framework, the chairman of COSO, Bob Hirth, graciously invited me to participate in an advisory committee chartered to update and improve the framework. The new framework is scheduled to be released in 2017 after a comment and revision period. Out of respect to the work of the advisory committee and working groups, I will reserve comment until the new framework is published in its final form. At this point, I will say that the new framework addresses many of my critical comments. In the rest of this section, I will refer to the 2004 framework.

The Structure The concept behind the COSO ERM framework is a set of four basic entity objectives (See Figure 7.5). The framework is a cube-shaped matrix that breaks down these objectives in terms of control components and the organization's business structure. One dimension of the framework provides four categories of entity objectives:

1. **Strategic:** high level, mission-oriented goals
2. **Operations:** effective and efficient resource usage
3. **Reporting:** reliable information and communication
4. **Compliance:** conformity to laws and regulations

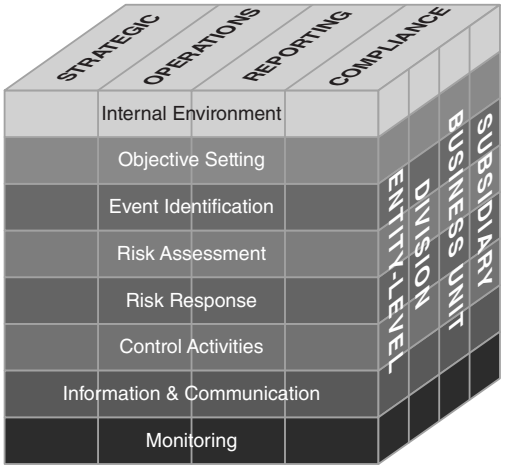

FIGURE 7.5 The COSO ERM Framework
"Enterprise Risk Management—Integrated Framework," *Committee of Sponsoring Organizations of the Treadway Commission*, September 2004

The second dimension of the framework is a list of eight ERM components. While these elements could be considered sequential, COSO avoids such a view, instead emphasizing their interconnected nature. These include:

1. **Internal Environment:** shaping company culture, ethical values, risk perception and appetite
2. **Objective Setting:** creating goals within the four categories listed above
3. **Event Identification:** distinguishing between internal and external risks and opportunities
4. **Risk Assessment:** evaluating risk based on likelihood and impact
5. **Risk Response:** deciding whether to avoid, accept, reduce, or share risk
6. **Control Activities:** establishing procedural precedent to ensure appropriate response
7. **Information and Communication:** capturing and sharing information to support informed decisions
8. **Monitoring:** continually evaluating and optimizing business and risk processes

Finally, there is a third dimension to the framework in which all four objectives and eight components above are broken down by the structural elements of the organization itself:

1. Entity-Level
2. Division
3. Business Unit
4. Subsidiary

The idea behind the framework is to create a complete taxonomy of risk management, permitting evaluation and analysis at a granular level. For example, how optimized is the company's risk assessment when it comes to operations at the business unit level? What is the division-level internal environment surrounding regulation compliance? As you can see, a full implementation of the COSO framework is both broad and detailed.

Current Use In 2010, about 55% of U.S. organizations of various sizes and in numerous industries were using the COSO framework, with only 2% using the next most popular one.[6] COSO is a leading voice when it comes to compliance with legal codes. When the United States passed the Sarbanes-Oxley Act of 2002, which expanded internal control requirements for public companies, COSO was quick to publish an updated internal controls framework that incorporated the new legislation.[7] Companies that use some version of the COSO framework include Newell Rubbermaid, Alliant Energy, Mirant, and TD Ameritrade.

The COSO ERM framework is especially popular among very large corporations and banks, which must comply with extensive legal codes and face particularly complex, high-stake risks. However, the complexity that draws large organizations to this framework can be an obstacle for small to mid-size companies. Of 460 organizations polled in 2010, over 76% had a moderate or significant concern that the framework was overly theoretical, while 26% felt that the cube illustration was unnecessarily complicated.[8]

Referring back to our five initial criteria for an ERM framework, COSO is neither simple nor MECE. Consider the overlap between control activities and risk response or between information and monitoring. What's more, the sheer size of the matrix inevitably results in numerous similar or identical cells. How does the intersection of reporting and objective-setting truly differ from the confluence of information and strategic objectives? While certain corporations may need that level of nuanced detail in their ERM processes, it is difficult to grasp and to communicate to stakeholders.

The COSO ERM framework is also not very flexible when it comes to evolving needs. It is designed to account for any possible eventuality or

change in business plan, so in that sense it has the potential to fit the needs of any business. But its rigid structure may result in a lot of management waste. It is like a one-size-fits-all life jacket: workable for big businesses, but awkward and unwieldy for smaller ones. And when it comes to a practical ERM model, we are looking for a well-tailored suit.

Nor is COSO as effective as it could be. The framework doesn't fully address the relationship between risk and reward. Remember that risk is a bell curve that indicates the relative probability of *all* outcomes, upside, downside, and neutral. The peak of the bell curve merely represents the likeliest of these outcomes. Visualizing risk in this manner offers opportunities to tweak the curve's shape to increase the likelihood of favorable results (for instance by reallocating resources) and reduce not only the likelihood of negative ones but their severity as well (for example, via risk transfer). With its strong emphasis on assessment and governance, COSO gives short shrift to actual risk *management*.

Finally, I have concerns about how many companies are using the COSO framework for their risk assessments. Most simply plot each risk against its probability and severity. While this has the virtue of simplicity, it essentially collapses the risk bell curve into a single point. Many companies compound this error by applying mathematics to their qualitative analyses, for example, multiplying severity rating by probability rating to create an overall risk "score." A healthcare company I once worked with had used an even more baffling equation: probability rating plus severity rating divided by 2. Their only reasoning? That a consultant had recommended that years before!

As discussed above, the new COSO framework will address many of these shortcomings. My purpose here is not to beat a dead horse. And the transition from the old to new framework will take time. Nevertheless, it is important for companies that are currently using the old framework to understand its potential pitfalls.

Australia-NZ Model (AS/NZS) aka ISO 31000

In 1995 a group of government and private-sector organizations from New Zealand and Australia assembled to develop and publish a generic and flexible model for risk management. They hoped that it could be adapted to fit the needs of any industry. Their efforts were successful, and the model slowly spread into the northern and western hemispheres. It was even revised and adopted by the International Organization for Standardization (as ISO 31000) in 2009.[9] The framework was updated slightly in 1999 and again in 2004.

The Structure Whereas COSO emphasized the interconnection of all aspects of risk management, the AS/NZS ERM model is a linear process

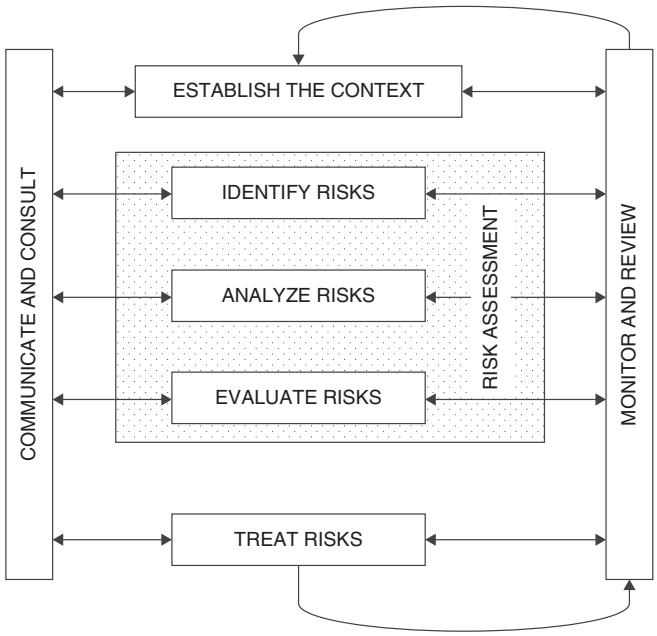

FIGURE 7.6 The Australia-NZ Model (ISO 31000)
Standard AS/NZS ISO 31000:2009, Risk Management—Principles and Guidelines

(see Figure 7.6). COSO urges a continual evaluation of one component in terms of the others; the AS/NZS model is cyclic and iterative. There are seven interconnected elements in the AS/NZS framework. The basic cycle of the model begins with establishing the risk context and progresses through identification, analysis, evaluation, treatment, and monitoring/reviewing before returning to establishing context. The monitoring and reviewing step also influences each stage of the ERM process, as does the first component of the framework, communicating and consulting.

1. **Communicate and Consult.** Communicating with internal and external stakeholders at each stage in the process is central to this model.
2. **Establish the Context.** Context includes business objectives, risk appetite, and criteria for evaluating risk.
3. **Identify Risks.** Identify where, when, why, and how events could prevent, degrade, delay, or enhance the achievement of business objectives.
4. **Analyze Risks.** Determine likelihood and consequences; identify and evaluate the effectiveness of existing controls.

5. **Evaluate Risks.** Prioritize risks by measuring them with the pre-established criteria and consider the potential benefits and adverse outcomes.
6. **Treat Risks.** Develop and implement specific cost-effective strategies and action plans for increasing potential benefits and reducing potential costs.
7. **Monitor and Review.** Monitor the effectiveness of the risk management program to ensure that it is operationally sound and cost-effective.

Current Use Like COSO, AS/NZS has found widespread use around the globe. In addition to ISO's version, nearly identical frameworks are in use by London's Institute of Risk Management, the U.S.-based Institute of Management Accountants, and the U.S. Department of Energy. As its designers intended, there is some variation among implementations. In fact, they considered the framework a template that each organization would fill out according to its needs.[10] The result is an intuitive structure based on a set of processes and principles applicable to any organization.

While the AS/NZS framework meets many of our criteria for a strong ERM framework, it could be more balanced. Three of the seven components have to do with risk assessment while there is very little guidance about actually dealing with risks or making risk-informed business strategy and policy decisions. The similarity among the three risk-assessment components (identify, analyze, and evaluate) makes it less MECE than we'd like.

Lam's ERM Framework (2003)

In my 2003 book, I recommended a model ERM framework that combined the simplicity of AS/NZS with the rigor of COSO. The structure consists of four interconnected layers, each with one to three elements for a total of seven components. See Figure 7.7 for my 2003 ERM framework. Let's examine the levels and components of that framework.

Level 1: Risk Governance

Corporate governance sits at the top of the entire framework. It ensures that the board of directors and management have established the appropriate organizational processes and corporate controls to measure and manage risk across the company.

Level 2: Risk Origination and Management

Line management integrates risk management into the revenue-generating activities of the company, including business development, product and relationship management, risk-based pricing, and so on.

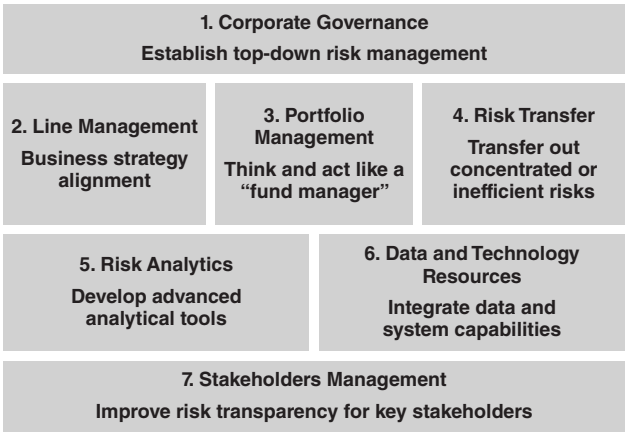

FIGURE 7.7 Lam's ERM Framework (2003)

Portfolio management aggregates risk exposures, incorporates diversification effects, and monitors risk concentrations against established risk limits.

Risk transfer mitigates risk exposures that are deemed too high, or are more cost efficient to transfer to a third party than to hold in the company's risk portfolio.

Level 3: Risk Analytics and Data Management

Risk analytics provides the measurement, analysis, and reporting tools to quantify the company's risk exposures as well as track external drivers.

Data and technology support the analytics and reporting processes.

Level 4: Communication and Relationship Management

Stakeholder management includes meeting stakeholder expectations and communicating and reporting the company's risk information to its key stakeholders. As with corporate governance, stakeholder management encompasses the breadth of ERM and serves as the model's foundation.

AN UPDATE: THE CONTINUOUS ERM MODEL

My own thinking has evolved since the publication of my first ERM book. Based on work with client organizations across various industries and

FIGURE 7.8 The Continuous ERM Model

different maturity levels, I've come to believe that a simplified framework, with no greater than 4–5 components, would be more intuitive and useful. The continuous ERM model I describe in Chapter 3 is a refinement of this earlier framework. Here, I've reduced the number of components from seven to four, and illustrate the cyclical, iterative nature of continuous ERM using feedback loops. Figure 7.8 shows the updated ERM framework. It is important to note that the four components specifically address four fundamental questions related to risk management:

1. **Governance structure and policies:** *Who* is responsible to provide risk oversight and make critical risk management decisions?
2. **Risk assessment and quantification:** *How* (ex-ante) will they make these risk management decisions in terms of analytical input?
3. **Risk management:** *What* specific decisions will they make to optimize the risk/return profile of the company?
4. **Reporting and monitoring:** *How* (ex-post) will the company monitor the performance of risk management decisions (i.e., a feedback loop)?

Governance Structure and Policies

Governance structure and policies address the question of who (i.e., individuals, functions, or committees) is responsible for making risk management decisions, and what policies provide incentives, requirements,

and constraints (e.g., risk tolerances) for the decision makers. Governance structure and policies should include the following:

Risk Governance How should the board provide effective risk oversight?

- Should the board consider establishing a separate risk committee, or assign risk oversight responsibility to the audit committee or the full board?
- Should the board consider adding a risk expert to assist in risk issues, similar to the addition of financial experts to oversee financial issues?
- Should board members be more engaged in the risk management process?

Companies should address these questions regarding the board's governance structure, risk expertise, and its role in ERM to enhance the board's effectiveness in providing risk oversight. As a recent example, UBS announced that it added one CRO and two CFOs to the board, and investors reacted favorably, sending the stock price up seven percent in late trading. At the same time, board members should be fully engaged in the risk management process. This includes debating risk tolerance levels, challenging management on critical business assumptions, and holding management accountable for the risk–return performance of past decisions.

ERM Policy Companies should establish an ERM policy to support the risk oversight activities of senior management and the board. One of the most important components of an ERM policy is the delineation of specific risk tolerance levels for all critical risk exposures, known as the risk appetite statement (RAS). These risk tolerance levels enable the board and corporate management to control the overall risk profile of the organization. Other key components of an ERM policy typically include:

- Board and management governance structure
- Summaries of risk committee charters
- Risk management roles and responsibilities
- Guiding risk principles
- Summaries of risk policies and standards
- Analytical and reporting requirements
- Exception management and reporting processes

Risk-Compensation Linkage The design of incentive compensation systems is one of the most powerful levers for effective risk management (including risk

culture), yet until very recently companies have paid insufficient attention to how incentives influence risk/return decisions. For example, when earnings growth or stock price appreciation drives incentive compensation, as is typical, corporate and business executives are effectively motivated to increase risks in order to drive up short-term earnings and stock price. To better align the interests of management and investors, long-term, risk-adjusted financial performance should drive incentive compensation systems. There are several ways to achieve this:

- Incorporating risk management performance into incentive compensation
- Establishing long-term risk-adjusted profitability measurement
- Using vesting schedules consistent with the duration of risk exposures
- Applying clawback provisions to account for tail risk losses.

Risk Assessment and Quantification

Risk assessment and quantification processes address the question of how analytical tools and processes support risk management decisions. Risk assessment and quantification tools for ERM include:

- **Risk assessments** that identify and evaluate the key risks facing the organization, including estimations of the probability, severity, and control effectiveness associated with each risk.
- **A loss-event database** to capture systematically an organization's actual losses and risk events so management can evaluate lessons learned and identify emerging risks and trends.
- **Key risk indicators (KRIs)** that provide measures of risk exposures over time. Ideally, KRIs are tracked against risk tolerance levels and integrated with related key performance indicators (KPIs).
- **Analytical models** that provide risk-specific and/or enterprise-wide risk analyses, including value-at-risk (VaR), stress-testing, and scenario analyses. One of the key objectives of these models is to provide loss estimates given an organization's risk portfolio.
- **Economic capital models** that allocate capital to underlying risks based on a defined solvency standard. These models often support risk-adjusted profitability and shareholder value analyses.

While the above tools can provide useful information, organizations should be aware of potential pitfalls. One of the key lessons from financial crises is that major risk events are usually the result a confluence of

interrelated risks rather than any single risk on its own. To avoid the silo approach to risk analysis, companies need to integrate their risk assessment and quantification processes, as well as focus on critical risk interdependencies. Currently, many companies employ valuable tools, but they are typically utilized independently rather than in a holistic manner. They may use value-at-risk models to quantify market risk, credit-default models to estimate credit risk, and risk assessments and KRIs to analyze operational risk. Going forward, companies must integrate these analyses to gain a broader perspective.

Risk models are only as reliable as their underlying assumptions. Prior to the financial crisis of 2008, many of the credit models used were based on the assumption that years of rising home prices and benign default rates would continue in the future. Moreover, credit and market risk models often assume some level of diversification benefits based on historical default and price correlations.

However, the financial crisis has also provided strong evidence of the risk management adage that price correlations approach one during market stresses (i.e., global asset prices dropped in concert). In other words, the benefit of diversification may not be there when it's needed most. Companies should stress-test the key assumptions of their risk models to understand how sensitive results are relative to these assumptions.

Risk Management

Risk management addresses the decisions and actions companies have to optimize their risk/return. As discussed in Chapter 3 and further elaborated in Chapter 16, key risk-response decision points include:

- Risk acceptance or avoidance
- Risk mitigation
- Risk-based pricing
- Risk transfer
- Resource allocation

Typically, the risk management function does not handle the above decisions, but rather supports business and corporate decision-makers by providing risk/return analyses and tools. Moreover, the risk function should offer an independent assessment of critical business/risk issues.

The role and independence of the risk management function is a critical issue. Should the risk function be a business partner and actively participate in strategic and business decisions, or take the role of a corporate overseer

and provide independent oversight? Can the risk function balance these two potentially conflicting roles? A related issue is whether the chief risk officer (CRO) should report to the CEO or to the board, or both.

One organizational solution may be to establish a solid reporting line between the CRO and CEO, and a dotted reporting line between the CRO and the board. On a day-to-day basis, the risk function serves as a business partner advising the board and management on risk management issues. However, under extreme circumstances (e.g., CEO/CFO fraud, major reputational or regulatory issues, and excessive risk taking) the dotted line to the board becomes a solid line such that the CRO can go directly to the board without concern about his or her job security. Ultimately, to be effective the risk function must have an independent voice. A direct communication channel to the board is one way to ensure that this voice is heard.

Reporting and Monitoring

The risk reporting and monitoring process addresses the question of how critical risk information is reported to the board and senior management, and how risk management performance is evaluated.

Currently, a general sense of dissatisfaction exists among board members and senior executives with respect to the timeliness, quality, and usefulness of risk reports. Companies often analyze and report on individual risks separately. These reports tend to be either too qualitative (risk assessments) or quantitative (VaR metrics). Risk reports also focus too much on past trends. In order to establish more effective reporting, companies should develop forward-looking, role-based dashboard reports, customized to support the decisions of the individual or group, whether that is the board, executive management, or line and operations management. ERM dashboard reports can integrate qualitative and quantitative data, internal risk exposures and external drivers, and key performance and risk indicators.

In order to evaluate the performance of the ERM program itself, organizations need to establish metrics and feedback loops based on measurable objectives. The objective of risk management could, for instance, be defined as to minimize unexpected earnings volatility. In this case, the purpose of risk management is not to minimize absolute levels of risks or earnings volatility, but to minimize unknown risks or drivers of earnings volatility.

DEVELOPING A FRAMEWORK

In addition to organizing the processes underpinning ERM, frameworks can be a powerful communication tool. This is particularly true in cases where the risk culture of an organization has not reached full maturity or, as is too

often the case, there is no real risk culture at all. For that reason, the first step in developing a workable ERM framework for one's organization is to assess not only the risk processes already in place, but also the current risk culture. Let's review some of the key risk culture drivers in light of how they might inform an ERM framework:

- **Risk awareness:** How are employees made aware of the risks involved in their day-to-day decision-making? And how can that process be improved? An efficient risk framework should enhance risk awareness.
- **People:** Who is in charge of disseminating risk-related information? Where do their roles intersect with the roles of decision-makers across the organization? The framework should provide guidance as to the necessary risk-related roles.
- **Skills:** Each component of the framework will require certain skills. Does the framework make those clear? What systems must be in place to develop these capabilities?
- **Integrity:** This speaks to how well employees and managers internalize risk awareness and response, which in turn is a product of how fully risk is integrated into key processes. The framework should, therefore, be closely integrated with the broader strategic framework of the organization, so that the two reinforce one another rather than conflict.
- **Incentives:** A framework should elucidate the behaviors that best support the risk management goals of the company. Incentive programs and compensation schemes should reinforce those behaviors.
- **Tone from the top:** In order for the company's board members, CEO, and other business leaders to express their commitment to risk management, that tone must be ingrained in the ERM framework. What's more, the framework should inform the roles that senior management and the board play in risk management.
- **Communication:** Is the ERM framework effective as a communication tool? Does it clarify the role of risk in day-to-day decision-making? And does it illuminate the lines of communication that must be open in order for ERM to be fully effective?
- **Change management:** While the framework itself will not directly address change management, it should offer some guidance as to how it might take place. For example, it would provide discrete components of ERM, some of which may be more challenging to implement than others. This could help prioritize where to begin with implementation.

Adapting the Continuous ERM Framework

The goal of the Continuous ERM Model is to capture the strengths of the frameworks above in a single template that is flexible enough to

accommodate the needs of organizations across industries. It is designed to meet the five criteria of an enduring framework: simplicity, MECE, balance and integration, flexibility, and effectiveness. Ultimately, it is a theoretical abstraction that should lead to real applications of ERM programs. For example, the application of this framework in a small non-profit is going to look very different from implementation in an international bank. It is important for the CRO (or equivalent position) to assess the needs of the organization, then choose and adapt an ERM framework that is tailored to those needs. The scope and complexity of the framework should match that of the organization. The components of the framework should be balanced to reflect the priorities of the organization. As the company works to adapt the framework to meet the organization's needs, it must keep in mind not only the aspects of risk culture discussed above, but also the "hard," numerical aspects of ERM. While the framework will not enumerate specific metrics used to measure performance, it will provide guidance as to what those metrics might be, and, more importantly, it will establish a reporting and monitoring structure to make sure those metrics and their accompanying analysis reach those who need them in a timely manner.

From Framework to Standards

As the company implements a framework, it will begin establishing precedents to inform best practices and goals to strive for as an organization. These can in turn form the basis for an ERM development roadmap. A clear vision for continual ERM improvement is key to staying ahead of the curve when it comes to risk. In order to do so, companies should use the framework to answer the following questions:

1. **Where are we?** The feedback loops and monitoring protocols established in the framework should reveal the current status of the organization's ERM efforts.
2. **What are the best-in-class practices to strive toward?** A good framework should help make apples-to-apples comparisons with competitors and even companies in other industries. Those comparisons, along with the knowledge gained from experience, should help evaluate where the organization could be based on its size, industry, and complexity.
3. **What do we need to do in order to reach our ideal state?** Once the risk team has established the starting point and goal, it can begin creating the roadmap: Do policies need updating? Does the risk culture need to change? Who must take action?

What does the process of establishing standards look like? Imagine this situation: A company uses a VaR model to determine market risk on a monthly basis as part of the risk assessment and quantification components of its framework. To take standards to the next level, the company can measure exposure more frequently. The best practice would be continuous, real-time monitoring, but this "Olympic-level" precision may not be necessary or cost-effective for less complex organizations, such as a regional bank. That's what I mean by customizing best practices based on the size and complexity of the organization. If daily measurement is sufficient, continuous monitoring would be overkill. This means that in order to achieve best-in-class practice, the company must shift from monthly to daily reporting. The ERM framework is a tool to close this gap. It allows companies to organize their current set of standards, get the needed reports, and create a roadmap to best-in-class practice.

CONCLUSION

In this chapter, we looked at how frameworks can offer a high-level view of key business processes such as strategic planning and execution. We examined the criteria that make a framework both simple enough to understand but flexible and sophisticated enough for large, complex organizations. Then, we focused our attention on the available ERM frameworks, including my own, the Continuous ERM Model. And finally, I discussed ways in which companies can adapt one or more of these models to fit their needs. Establishing such a framework is the first step in creating an ERM program. It is the cornerstone upon which companies will build out a comprehensive risk management approach that will inform every aspect of decision-making and strategic direction.

NOTES

1. Reeves, Martin, Moose, Sandy, and Venema, Thijs. "BCG Classics Revisited: The Growth Share *Matrix*," Boston Consulting Group, 2014. Retrieved from https://www.bcgperspectives.com/content/articles/corporate_strategy_portfolio_management_strategic_planning_growth_share_matrix_bcg_classics_revisited/.
2. Porter, Michael E. *Competitive Strategy: Techniques for Analyzing Industries and Competitors*, Free Press, 1998.
3. Kaplan, Robert S. and David P. Norton. "The Balanced Scorecard—Measures that Drive Performance," *Harvard Business Review*, January–February 1992.
4. Moore, Geoffrey. *Zone to Win: Organizing to Compete in an Age of Disruption*, Diversion Books, 2015, pp. 34–37.

5. *Enterprise Risk Management—Integrated Framework*. Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2004. Retrieved from www.coso.org.
6. Beasley, Mark, Bruce Branson and Bonnie V. Hancock. *COSO's 2010 Report on ERM: Current State of Enterprise Risk Oversight and Market Perceptions of COSO's ERM Framework*, Organizations of the Treadway Commission (COSO), 2010.
7. Ibid.
8. Ibid.
9. *ISO 31000: Risk Management*, ISO, 2015 *Joint Technical Committee OB-007 Risk Management*. Risk Management Standards, Standards Australia International and Standards New Zealand, 1995
10. Ibid.