Association for Financial Professionals®

AFP

RISK MANAGEMENT

The ERM Guide from AFP

WRITTEN BY
James Lam

Advisory Statement

This Guide is intended to provide a framework from which enterprise risk management (ERM) programs can be developed. The Guide is best used as an overall benchmark of industry best practices that can help a company to plan, develop, and improve its ERM processes.

The Guide is not intended to be, nor should it be considered, a complete step-by-step resource to mitigate an organization's risks. Rather, it is designed to provide practical guidance with respect to the business rational and specific requirements for implementing an ERM program.

As it is not possible to reference in this Guide all applicable aspects of legislation and regulation related to governance, risk and compliance activities, it is important that readers take appropriate actions to understand the governance and compliance issues that face their business. Appropriate actions may include retaining external service organizations to provide advice and guidance in the development of programs, and independent review services for implemented programs.

About the Author

James Lam is President of James Lam & Associates, a Boston-based consulting firm that is singularly focused on risk management. He is widely regarded as the first "chief risk officer" and an early advocate of enterprise risk management. Mr. Lam provides board advisory, management consulting, and executive training services. A Forrester Report "Identifying and Selecting the Right Risk Consultant" ranked James Lam & Associates among a select number of consulting firms with "extensive risk capabilities" across all major industries.

Over his consulting career, Mr. Lam has successfully completed over 100 risk management engagements and achieved an exceptionally high level of client satisfaction. In a Euromoney survey, he was nominated by clients and peers as one of the leading risk consultants in the world. Mr. Lam is the author of *Enterprise Risk Management: From Incentives to Controls*, which has ranked #1 best selling among 25,000 risk management titles on Amazon.com. The book has been translated into Chinese, Indonesian, Japanese, and Korean. In 1997, Mr. Lam received the inaugural Risk Manager of the Year Award from the Global Association of Risk Professionals. Treasury & Risk magazine named him one of the "100 Most Influential People in Finance" in 2005, 2006, and 2008.

In addition to this Guide, Mr. Lam has worked with AFP to develop and deliver a range of risk management courses to its members.

ERM Definitions and Concepts

How is ERM defined? It depends on who you ask. A more relevant question may be how ERM *should* be defined at your organization. That depends on what you want to accomplish with your ERM program. For any organization developing or implement ERM, it is important to establish a standard definition regardless if that definition is adopted from a published source or customized for the specific objectives of the organization.

Let's review three published definitions of ERM and some of the key concepts embedded in those definitions.

In May 2003, the following definition was published in *Enterprise Risk Management: From Incentives to Controls*, a Wiley Finance book written by this author:

> **"ERM is an integrated framework for managing credit risk, market risk, operational risk, economic capital, and risk transfer in order to maximize firm value."**

In September 2004, the following definition was published in *Enterprise Risk Management: Integrated Framework* by the Committee of Sponsoring Organizations of the Treadway Commission (COSO):

> **"ERM is a process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."**

In November 2009, the following definitions were published in *ISO 31000: 2009 Risk Management* by the International Organization of Standardization (ISO):

> **Risk is the "effect of uncertainty on objectives" and risk management is "coordinated activities to direct and control an organization with regard to risk."**

A review of the above definitions and related materials would highlight the following key concepts in ERM:

1. **Managing uncertainty**. "Expect the unexpected" is a risk management mantra. More than ever, organizations face a high degree of uncertainty in the economic and business environment. To survive and prosper, an organization must manage its key risks within a defined risk appetite.
2. **Integrated framework**. ERM is all about integration. It should provide integrated analyses, integrated strategies, and integrated reporting with respect to an organization's key risks and interdependencies.
3. **Strategy and business setting**. ERM should be integrated into a firm's strategy and business management processes including business strategy, product pricing, risk transfer, capital allocation, and incentive systems.
4. **Tone from the top**. ERM should be directed by the firm's board of directors, corporate executives, and other business leaders. The engagement of business leaders in the ERM process is a key success factor in influencing an organization's risk culture.
5. **Value added**. ERM should not be focused narrowly on regulatory compliance or loss minimization. It should also enhance an organization's ability to achieve business objectives and maximize firm value.

ERM Trends and Drivers

In the aftermath of the global financial crisis, ERM has emerged as a critical issue for organizations across different industry sectors. Recent surveys have indicated that managing risk has become the top agenda item for corporate directors and executives. While ERM has gained wider attention and acceptance, most organizations are still in the early stages of development and implementation. In a 2010 COSO ERM survey, only 28 percent of respondents described their ERM process as "systematic, robust and repeatable with regular reporting to the board." Other surveys confirm that only a small minority of organizations would describe their ERM programs as being fully developed and implemented. Clearly, there is significant work to be performed to at most organizations.

What are the key drivers for ERM? Let's examine five current trends that underpin the global adoption of ERM practices.

- **Financial and corporate disasters.** The global financial crisis represented a dramatic and painful wake-up call with respect the consequences of ineffective risk management. At the 2009 World Economic Forum, it was reported that at its peak the global financial crisis destroyed 40-45% of world wealth. The crisis resulted in several of the biggest U.S. corporate bankruptcies in history, including Lehman Brothers, Washington Mutual, and General Motors. Many firms had to be bailed out by the U.S. Government to avoid bankruptcy, and few businesses were left unscathed. One key lesson learned is that major disasters are often caused by a confluence of risk events, and that organizations need to manage risks and their independencies on a comprehensive and integrated basis. With this lesson in mind, organizations have reexamined their ERM processes to identify key areas of improvement. These improvement areas include:
  - Board risk governance, oversight and reporting
  - Risk policies with explicit risk tolerance levels
  - Integration of ERM into business processes
  - Risk analytics and dashboards, with a focus on liquidity, counterparty, and systemic risks
  - Assurance and feedback loops on risk management effectiveness
  - Risk culture, including change management processes
  - Alignment of executive compensation and risk management objectives

  We will discuss these and other challenges in greater detail in the rest of the Guide.
- **Regulatory requirements**. In response to the corporate disasters, regulators have established more stringent governance and risk standards, as well as new examination, regulatory capital, and disclosure requirements. Some of the recent developments include:
  - In December 2009, the SEC established new rules that require disclosures in proxy and information statements about the board governance structure and the board's role in risk oversight, as well as the relationship between compensation policies and risk management.
  - In July 2010, the Dodd-Frank Act was signed into law. The Act requires a board risk committee be established by all public bank holding companies (and public non-bank financial institutions supervised by the Federal Reserve) with over $10 billion in assets. The board risk committee is responsible for ERM oversight and practices, and its members must include "at least one risk management expert having experience in identifying, assessing, and managing risk exposures of large, complex firms."
  - In September 2010, the Basel Committee on Banking Supervision announced a new global regulatory framework on bank capital adequacy. Basel III calls for higher capital requirements, including leverage limits and capital buffers, greater risk coverage includ-

ing counterparty risk and model risk, and minimum liquidity ratio.

The consequences of these and other regulatory requirements go beyond publicly-traded companies and financial institutions. As seen in the global impact of Sarbanes-Oxley, these requirements will have far-reaching influence on regulatory standards and risk management practices.

- **Industry initiatives**. Beyond regulatory requirements, a number of industry initiatives have established clear governance and risk standards around the world. The Treadway Report (United States, 1993) produced the COSO framework of internal control, while the Turnbull report (United Kingdom, 1999) and the Dey Report (Canada, 1994) developed similar guidelines. It is noteworthy that the Turnbull and Dey reports were supported by the stock exchanges in London and Toronto, respectively. Moreover, the Toronto Stock Exchange requires listed companies to report on their enterprise risk management programs annually. More recently, COSO published *Enterprise Risk Management: Integrated Framework* (2004). The International Organization for Standardization published *ISO 31000:2009 Risk Management* (2009). The National Association of Corporate Directors published *Risk Governance: Balancing Risk and Reward* (2009). These industry initiatives have gained significant attention from corporate directors and executives. Collectively, they provide a significant body of work on the key principles, standards, and guidelines for ERM.
- **Rating agencies and investors**. Other key stakeholders have espoused the merits of ERM. In 2008, Standard and Poor's (S&P) started to incorporate ERM assessments into its corporate rating processes. While less formalized than S&P, the other rating agencies (Moody's, Fitch, A.M. Best) are also increasing their focus on risk management capabilities as part of their rating processes. Equity analysts and institutional investors are paying more attention to ERM. Debt and stock analysts recognize the important role that ERM plays in a firm's creditworthiness and valuation. Given the lack of risk transparency during the global financial crisis, it is likely that rating agencies, stock analysts, and institutional investors will demand more timely and detailed disclosures on a firm's major risk exposures and ERM practices.
- **Corporate programs**. Ultimately firms will not continue to invest in ERM unless they see potential value. In this regard, corporations have reported significant benefits from their risk management programs, including stock price improvement, debt rating upgrades, early warning of risks, loss reduction, and regulatory capital relief. In addition to anecdotal evidence and published reports, there is a growing body of empirical studies that have associated superior financial performance and stock valuation with better corporate governance and ERM practices (see the next section on Creating Value through Governance and ERM Practices). Advanced ERM organizations see their programs as a competitive advantage that helps them mitigate complex risks and achieve business objectives.

Creating Value through Governance and ERM Practices

In terms of value creation, there is a large body of empirical research and survey data that would indicate companies with effective governance, risk, and compliance programs are associated with higher levels of profitability and market valuation. In recent years, governance and risk topics have received significant attention not only from the media, but also researchers. As a result, numerous research projects and surveys have been completed to evaluate the impact of sound governance and risk practices on company performance. While using different re-

search methodologies, sample size, and time periods, the key research studies and surveys have indicated that companies that have adopted better governance and ERM practices are associated with higher levels of profitability and market valuation. The following provides a synopsis of several key studies:

- McKinsey and Company (2002) surveyed over 200 institutional investors in 31 different countries with a combined $9 trillion of assets under management. They found that the large majority of investors were willing to pay a premium for companies with effective corporate governance practices. In North America, 76% of investors were willing to pay an average premium of 12-14% of market value.
- Cremers and Nair (2003) investigated how internal governance mechanisms interacted with external governance mechanisms. Based on equity prices from 1990 to 2001, they found that a portfolio with strong internal and external governance produced excess annualized returns of 8%. The same companies achieved 5.5% higher ROA (return on assets).
- Gompers, Ishii, and Metrick (2003) constructed a "Governance Index" based on 24 governance rules to measure the level of shareholder rights at about 1,500 large firms. They found that during the 1990s, an investment strategy that bought firms with the strongest rights and short firms with the weakest rights would have earned excess annualized returns of 8.5% during that period.
- Brown and Caylor (2004) analyzed the relationship between corporate governance and company performance. They found that firms with better governance achieve better financial performance, including higher return on equity (9.2% above industry average), higher profit margin (46% above industry average), and higher dividend payout (0.4% above industry average).
- Cheng and Wu (2005) and their research team at Institutional Shareholder Services examined the correlation between the ISS' Corporate Governance Quotient ratings and 16 financial performance metrics for more than 5,200 U.S. companies in the 2002-2004 period. They found that companies with better corporate governance have lower risk, better profitability and higher valuation. They found that that the top decile companies performed significant better than the bottom decile companies, including 3-to-10% versus negative return on assets; 8-to-15% versus 0.3% return on equity; and 16-to-20% vs. 10-to-15% stock price to earnings ratio.
- Hoyt and Liebenberg (2009) analyzed the relationship between the use of enterprise risk management (ERM) processes and firm value. To control for regulatory and market differences across industries, the researchers focused on publicly-traded U.S. insurance companies. They quantified a 16.5% "ERM premium," or a positive and statistically significant relationship between firm value and the use of ERM.
- Deloitte (2011) surveyed 131 global financial institutions with more than $17 trillion in total assets. When asked about the cost-benefit of their ERM efforts, 85% indicated that the value of their ERM program was greater than its cost.

Based on the empirical and survey data provided above, it is clear that the implementation of effective governance and ERM processes can add measureable value to firms. In the next section, we will examine the fundamental requirements for an ERM framework.

Key Components of an ERM Framework

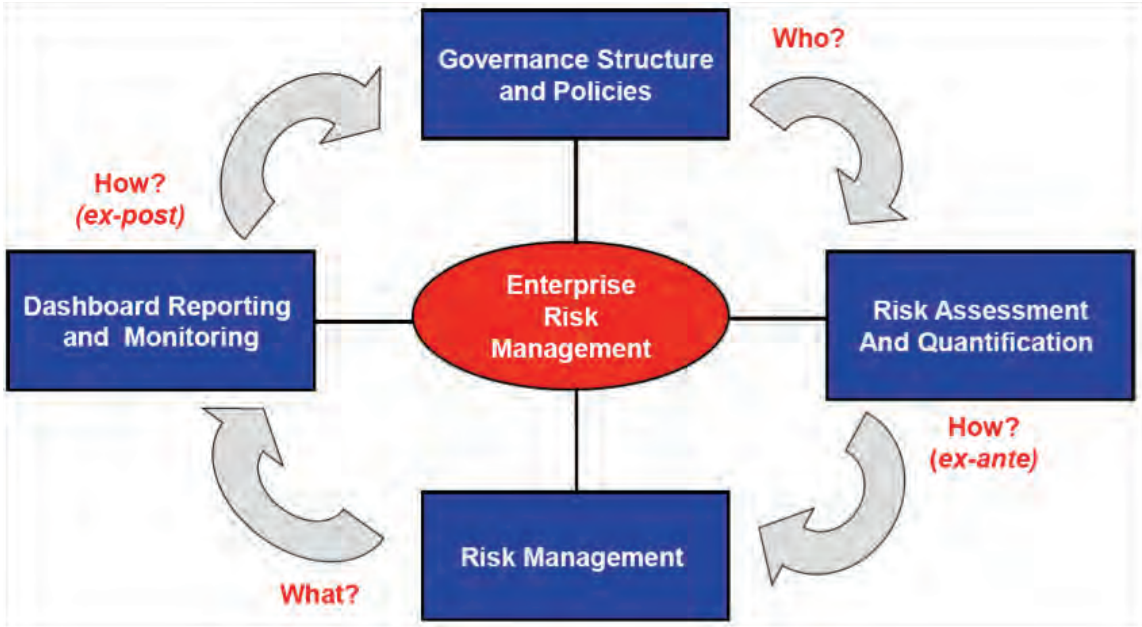
Any organization implementing ERM should develop an overall framework to ensure that the fundamental requirements are addressed. The decision is generally to either adopt a published framework (e.g., COSO ERM, ISO 31000) or develop a customized framework based on the unique require-

ments of an organization. Regardless, any ERM framework must address four fundamental issues, as shown in Figure 1. Each of the four components addresses a key question:

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

The above questions may sound simple but addressing them effectively can be very challenging for most firms. However, an effective ERM framework must address all four of these issues.

Figure 1: ERM Framework



Source: James Lam & Associates

Governance Structure and Policies

Governance structure and policies address the question who (i.e., individuals or committees) is responsible to make risk management decisions, and what are the policies that provide incentives, requirements and constraints (e.g., risk tolerances) for the decision makers. Governance structure and policies should including the following:

- **Risk governance**. How should the board provide effective risk oversight? First, should the board consider establishing a separate risk committee, or assign risk oversight responsibility to the audit committee or the full board? Second, should the board consider adding a risk expert to assist in risk issues, similar to the additions of financial experts to oversee financial issues? Finally, should board members be more engaged in the risk management process? These questions regarding the board's governance structure, risk expertise, and its role in ERM, should be addressed to enhance the board's effectiveness in providing risk oversight.
- **ERM Policy**. To support the risk management oversight activities of the board, an ERM policy should be established. Key components of an ERM policy may include board and management governance structure, summary of risk committee charters, risk management roles and responsibilities, guiding risk principles, summary of risk policies and standards, analytical and reporting requirements, and exception management processes. Moreover, one of the most important components of an ERM policy is specific risk tolerance levels for all critical risk exposures. These risk tolerance levels enable the board and corporate management to control the overall risk profile of the organization.
- **Risk-compensation linkage**. The design of incentive compensation systems is one of the most powerful levers for effective risk management, yet insufficient attention has been paid to how incentives influence risk-return decisions. For example, if incentive compensation is driven by earnings growth or stock price appreciation, then corporate and business executives would be motivated to increase risks in order to drive up short-term earnings and the stock price. Traditional executive compensation systems do not provide the appropriate framework for risk management because they can motivate excessive risk taking. To better align the interests of management and investors, incentive compensation systems must be driven by long-term, risk-adjusted financial performance. This can be achieved by incorporating risk management performance into the incentive compensation system; establishing long-term risk-adjusted profitability measurement; using vesting schedules consistent with the duration of risk exposures; and applying clawback provisions to account for tail-risk losses.

Risk Assessment and Quantification

Risk assessment and quantification processes address the question 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. [For more information, see the AFP Risk Assessment Guide].
- Loss-event database that systematically captures 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, the KRIs are tracked against risk tolerance levels and integrated with related key performance indicators (KPIs).

- Risk 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 estimations 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 consequence of not one risk, but a confluence of interrelated risks. 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 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. However, each of these tools might be used independently. 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, 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 you need it most. Companies should stress-test the key assumptions of risk models to understand how sensitive model results are relative to these assumptions.

Risk Management

Risk management addresses the question what specific decisions are made to optimize the risk/return profile of the company. Key decision points include:

- **Risk acceptance or avoidance**. The organization can decide to increase or decrease a specific risk exposure through its core business, M&A, and financial activities.
- **Risk mitigation**. An organization can establish risk-control processes and strategies in order to manage a specific risk within a defined risk tolerance level.
- **Risk-based pricing**. All firms take risks in order to be in business, but there is only one point at which they can get compensated for the risks that they take. That is in the pricing of their products and/or services, which should fully incorporate the "cost of risk."
- **Risk transfer**. An organization can decide to execute risk transfer strategies through the insurance or capital markets if risk exposures are excessive and/or if the cost of risk transfer is lower than the cost of risk retention.
- **Resource allocation**. An organization can allocate human and financial resources to business activities that produce the highest risk-adjusted returns in order to maximize firm value.

At most organizations, the risk management function does not make the above decisions. Rather, they are made by business units and other corporate functions. However, the risk function should support business and corporate decision makers with the risk/return analytical tools outlined in the previous section. Moreover, the risk function should provide an independent assessment of critical business/risk issues.

The role and independence of the risk management function is a critical issue that should be addressed by each organization. Should the risk function be a "business partner" and actively participate in strategic and business decisions, or a "corporate overseer" and

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

One organizational solution may be to establish a solid line reporting between the CRO and CEO, and a dotted line reporting 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.

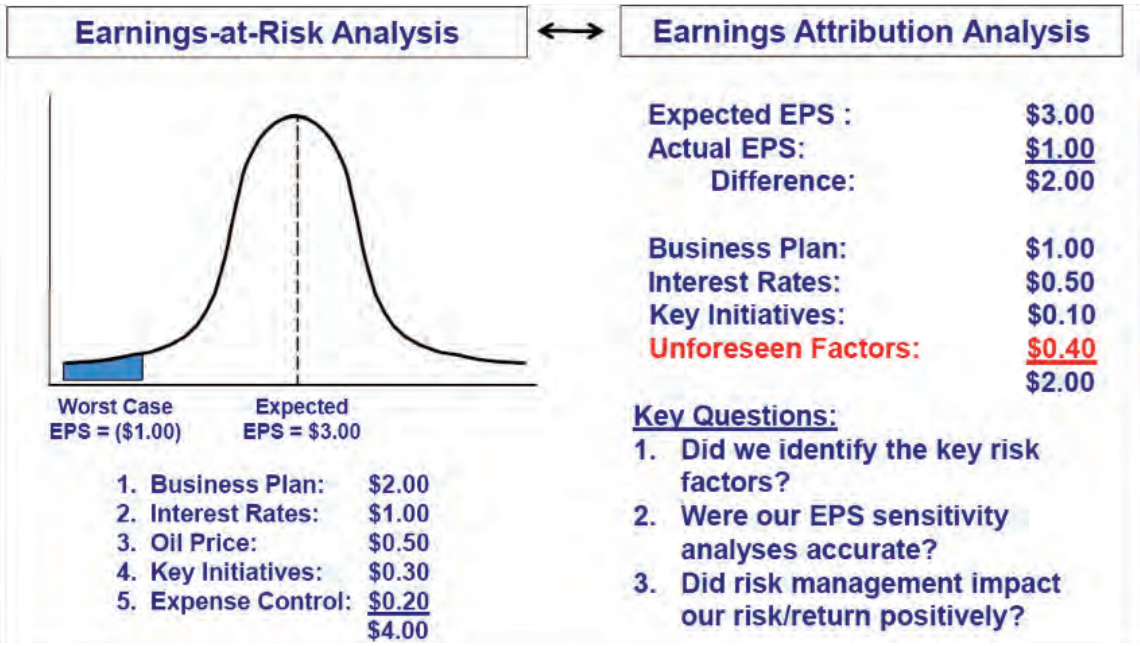
Reporting and Monitoring

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. It has been wisely said that what gets measured gets managed.

However, there is a general sense of dissatisfaction among board members and senior executives with respect to the timeliness, quality, and usefulness of risk reports. Currently, 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. These reports should be 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 should integrate qualitative and quantitative data, internal risk exposures and external drivers, and key performance and risk indicators.

How do we know if risk management is working effectively? This is perhaps one of the most important questions facing boards, executives, regulators, and risk managers today. The common practice is to evaluate the effectiveness of risk management based on the achievement of key milestones, or the lack of policy violations, losses, or surprises. However, qualitative milestones or negative proves should no longer be sufficient. Organizations need to establish performance metrics and feedback loops for risk management. Other corporate and business functions have such measures and feedback loops. For example, business development has sales metrics, customer service has customer satisfaction scores, HR has turnover rates, etc. In order to establish a feedback loop for risk management, its objective must first be defined in measurable terms. For example, the objective of risk management can be defined as to minimize unexpected earnings volatility. In other words, the objective of risk management is not to minimize absolute levels of risks or earnings volatility, but to minimize unknown sources of risks or earnings volatility. Based on this definition, Figure 2 provides an illustrative example of using earnings volatility analysis as the basis of a feedback loop. In the beginning of the reporting period, the company performs earnings-at-risk analysis and identifies several key factors (business targets, interest rates, oil price, etc.) that may result in a $1 loss per share, compared to an expected $3 earnings per share. At the end of the reporting period, the company performs earnings attribution analysis and determines the actual earnings drivers. The combination of these analyses provides an objective feedback loop on risk management performance. Over time, the organization strives to minimize the earnings impact of unforeseen factors. While this may not be the right feedback loop for an individual organization (i.e. non-profit), every company should establish some feedback loop(s) for risk management.

Figure 2: Earnings Volatility Analysis



Source: James Lam & Associates

Role of the Board in ERM

How should boards ensure that they play a constructive and effective role in ERM? Board members are not involved in day-to-day operations, and they have limited time to review materials and meet with management. What can they do to effectively oversee ERM and the key risks facing the organization? The role of the board in ERM encompasses three key levers: (1) establish an effective governance structure to oversee risk, (2) approve and monitor an ERM policy that provides explicit risk tolerance levels, and (3) establish assurance processes to ensure that an effective ERM program is in place. In academia, the acronym G.P.A. means grade point average. In the context of board risk oversight, the same acronym can be used to remember these three key levels: governance, policy, and assurance.

Governance

A fundamental step in providing ERM oversight is to establish an effective risk governance structure at the board level. Beyond an organizational chart, risk governance establishes the oversight roles and decision points for the board and board committees, as well as the relationships with management and management committees. In order to strengthen risk governance at the board level, organizations should consider adopting the following ERM practices:

- **Establish a risk committee**. While the full board generally retains overall responsibility for risk oversight, a growing number of organizations are establishing risk committees. Based on a survey of over 200 board members, a December 2010 report commissioned by COSO (COSO Report), 47% of board members at financial services organizations indicated that they had a risk committee, versus 24% at non-financial firms. Given the Dodd-Frank Act, and other regulatory reform, it is likely that these percentages will increase in the next few years. Regardless of the committee structure, the risk oversight roles of the full board and subcom-

mittees (e.g., audit, governance, HR) should be clearly defined. Boards should also ensure that they can effectively challenge management on risk management issues, by appointing board members and/or board advisors with deep risk management expertise and providing general risk education to all board members.

- **Align board and management structures**. The risk governance structures at the board and management levels should be fully aligned. This alignment includes committee charters, roles and responsibilities, reporting relationships, approval and decision requirements, and information flows. As boards become more active in establishing risk policies and risk appetite, the role of the board versus the role of management should be clearly differentiated. Figure 3 provides an example of the separation between management and board responsibilities for ERM. Alignment and clarification of roles would prevent unnecessary tensions and encroachments between management and the board.
- **Integrate strategy and risk**. Monitoring an organization's strategy and execution has long been the purview of boards. However, according to the COSO Report less than 15% of board members indicated that they were fully satisfied with the board's processes for understanding and challenging the assumptions and risks associated with the business strategy. However, a number of studies—James Lam & Associates (2004), Deloitte Research (2005), and The Corporate Executive Board (2005)—have found that strategic risks represented approximately 60% of the root causes when publicly-traded companies suffered significant market value declines, followed by operational risks (approximately 30%) and financial risks (approximately 10%). As boards become more active in ERM, the integration of strategy and risk is a logical and desirable outcome.

Figure 3: Management and Board Roles in ERM

ERM Component	Executive Management	Board of Directors
Risk Governance	Establish management structure and roles	Establish board structure and roles
ERM Vision and Plan	Develop and implement	Support vision; track progress against plan
Risk Tolerance Levels	Establish and conform	Debate and approve
Risk Policies	Develop and implement	Approve and monitor
Business and Risk Strategies	Formulate and execute	Challenge key assumptions; monitor execution
Critical Risks	Manage and measure; optimize risk/return	Provide input and oversight
Risk Reports	Provide context, analysis, and key points	Monitor key exposures, exceptions, and feedback loops
Risk Analytics	Provide qualitative and quantitative analyses	Obtain ERM assurance; conduct board assessments

Source: James Lam & Associates

Policy

While risk governance provides the organization for risk management and oversight, the board needs an instrument to communicate its expectations and requirements. Board-approved policies represent a critical tool in this regard. As shown in Figure 3 management's responsibility to develop and execute risk management policies. The board's role is to approve the policies and monitor ongoing compliance and exceptions.

An ERM policy may include the following components:

- **Executive Summary**. The executive summary provides a concise description of the purpose, scope and objectives for ERM. It may also provide a high-level summary of the key risk limits and/or risk tolerance levels.
- **Statement of Risk Philosophy**. The statement of risk philosophy discusses the overall approach to risk management. It may also include guiding risk principles that articulate the desired risk culture of the organization.
- **Governance Structure**. The governance structure section summarizes board committees and charters, management committees and charters, and roles and responsibilities. Moreover, the delegation of authority, including individual risk management and oversight responsibilities, should be documented.
- **Risk Tolerance Levels**. This section provides a statement of risk appetite, including specific risk limits or risk tolerance levels for critical risk exposures. It also provides exception management and reporting requirements.
- **Risk Framework and Processes**. This section summarizes the ERM framework, as well as key processes and specific requirements for overall risk management.
- **Risk Policy Standards**. This section establishes standards for other risk policies (e.g., credit risk policy, hedging policy, etc.) so that key risk policies are consistent across the organization.
- **Risk Categories and Definitions**. This section provides a risk taxonomy for commonly used terms and concepts so that a common language is used for risk discussions.

In addition to risk policies, the linkage to compensation policies should be a top board issue. As one observer remarked "people don't do what you tell them to do, they do what you pay them to do." As such, the board should ensure that risk management performance is considered in a meaningful way (20% weighting or more) in executive performance evaluations and incentives. These considerations may be specific risk management goals or an ERM scorecard that includes various quantitative and qualitative indicators. Regardless, by incorporating ERM into executive management incentives the board can have far-reaching impact on not only management behavior, but also the incentives and actions of all employees.

Assurance

While risk policies articulate board requirements for ERM, the board still needs information and feedback. How does the board know if risk management is working effectively? The answer lies in the assurance processes established by the organization, including board monitoring and reporting, independent assessments, and objective feedback loops.

In order to fulfill its mandate to oversee ERM, the board must rely on management to provide critical information with respect to board communications and reports. Board members often criticize the quality and timeliness of board reports. The standards that they want (but not getting to their satisfaction or not getting at all) include (a) a concise executive summary of business/risk performance, including the key decision points for the board, (b) management narrative on critical issues and trends, (c) key performance and risk indicators against specific targets or limits, and (d) more discussion with, versus presentation from, management. Recently, James

Lam & Associates worked with a large financial institution to improve its board communication and reporting. In addition to adopting these standards, the financial institution developed an ERM dashboard distributed through an iPad that provides high-level charts as well as drill-down capability to underlying data.

As boards retain independent auditors to review and assure the financial statements, they should retain an independent party to review and assure the ERM program. The final product of this review may be an assessment of the organization's ERM program relative to industry best practices and/or its development against plan.

Finally, the board should establish effective feedback loops to gauge the effectiveness of its ERM program. In the previous section, the use of earnings volatility analysis as a feedback loop on ERM was discussed. Regardless of the metric, the board should decide on the appropriate feedback loop(s) for risk management.

Key Success Factors in ERM

In this Guide we have discussed (1) basic definitions and concepts for ERM, (2) major trends and drivers for adoption, (3) evidence that ERM can create value, (4) the key components of an ERM framework, and (5) the role of the board in ERM. To review the key points discussed as well as look ahead with respect to the challenges in ERM implementation, let's examine seven key success factors:

1. **Board risk governance and reporting**. Perhaps the most powerful but underleveraged component in ERM is the role of the board. Boards wield significant influence over policy decisions and management actions. Executive teams go to great lengths to address issues raised by directors. As such, directors can have a significant impact simply by asking tough questions or requesting key risk reports.
2. **ERM policy with explicit risk tolerance levels**. The ERM policy is an important tool for both the board and executive management. The articulation of explicit risk tolerance levels for critical risks represents an essential element of the ERM policy. Given their importance in controlling the overall risk appetite of the organization, there should be sufficient discussion (and even debate) between the board and management before risk tolerance levels are established.
3. **ERM integration**. In order to optimize the organization's risk/return profile, ERM must be integrated into key business processes (e.g., product development and pricing, risk transfer, capital allocation). Another challenge is the integration of ERM and strategy. We discussed studies that have shown both the importance and the lack of understanding of strategic risks. While the integration of ERM and strategy is critical, this process is still in its early stages of development.
4. **Risk analytics and dashboards**. The consequences of the global financial crisis revealed some key shortcomings of existing risk analytical models. Commonly used risk models (e.g., value-at-risk, economic capital) only measure risks within a defined probability level, say 95% or 99%. However, organizations have learned that they must also prepare for "black swans," or highly improbable but consequential events. Going forward, risk analytics must be expanded to include stress testing and scenario analysis to capture "tail risk" events. Additionally, risk dashboards should be developed to provide forward-looking risk analysis as well as early-warning indicators.
5. **Assurance and feedback loops**. How do we know if risk management is working effectively? This is one of the most important questions facing boards, executives, regulators, and risk managers today. In the past, the common practice was to evaluate the effectiveness of risk management based on the achievement of key milestones, or the lack of policy violations, losses, or surprises.

However, qualitative milestones or negative proves should no longer be sufficient. Organizations need to clearly define the objectives of ERM and establish the appropriate performance metrics and feedback loops.

6. **Culture and change management**. The risk culture of an organization, and how to shape it, is an issue that is often overlooked in ERM. Moreover, the risk culture of an organization is not constant. It changes with the business environment, such new executive leadership, new incentives, or new risk processes and systems. Therefore, organizations should implement change management programs to build consensus, resolve conflicts, and provide ongoing communication and training.
7. **Risk and executive compensation**. A key driver of management behavior is the design of executive compensation systems. A root cause for the excessive risk-taking that led to the global financial crisis is executive compensation systems that reward short-term earnings growth and stock price appreciation. The design of incentive programs that reward long-term earnings growth, as well as risk management effectiveness, is a key initiative for many organizations today. These new incentive systems incorporate risk-adjusted return metrics, compliance with risk policies and regulations, longer-term vesting schedules, and clawback provisions in the event of future unexpected losses.

Summary

The development and implementation of an ERM program is a multi-year effort that requires significant commitment from the board and senior management. As a tool to help the reader gauge the development of ERM at his or her organization, we provided an ERM Maturity Model in the Appendix. The ERM Maturity Model will enable organizations to self-assess the maturity of their ERM programs, as well as identify opportunities to make further improvements. While the practice of ERM has evolved and matured significantly over time, there are critical challenges discussed in this Guide that need to be addressed. Without successfully addressing these challenges, the promise of ERM will continue to be unfulfilled. Finally, ERM is a journey and not a destination. For risk-intensive organizations, it has been, and will continue to be, a valuable journey.

Selected References

AFP Risk Assessment Guide, Association for Financial Professionals, 2011

COSO's 2010 Report on ERM, by Mark Beasley, Bruce Branson, and Bonnie Hancock, December 2010

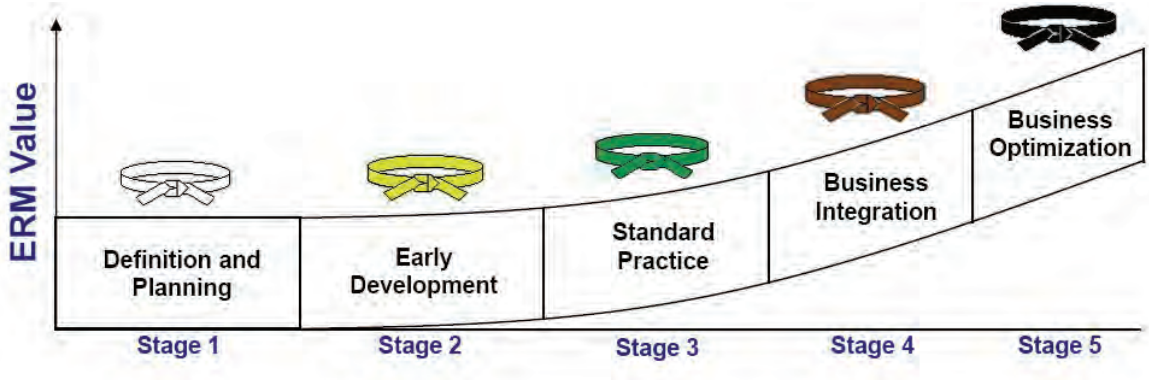
Enterprise Risk Management – From Incentives to Controls by James Lam, John Wiley & Sons, May 2003

Enterprise Risk Management: Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission, September 2004

Appendix: ERM Maturity Model

The purpose of the ERM Maturity Model is to provide useful industry benchmarks of ERM practices so readers can self-assess the maturity and development opportunities of their ERM programs. Since these are general industry benchmarks, it is possible that an organization may have specific ERM practices from a more advanced stage before completing all of the practices in prior stages. This reflects the fact that the development and evolution of ERM is unique to each organization.

The ERM Maturity Model



Source: James Lam & Associates

Stage 1: Definition and Planning (White Belt)

In Stage 1 the organization is organizing resources to define the scope and objectives for its ERM program. Key objectives during this phase include identifying an organization's ERM requirements, obtaining board-level and executive support, and developing an overall framework and plan for ERM. Some organizations find it useful to establish a cross-functional taskforce in order to accomplish these objectives. Stage 1 may take 6-12 months to complete and activities typically include:

- Researching regulatory requirements and industry practices
- Providing risk briefings for board members and corporate executives
- Appointing a chief risk officer and/or ERM project leader
- Organizing an ERM task force and/or ERM committee
- Conducting a benchmarking exercise with other companies
- Assessing the current state of risk management capabilities
- Defining the scope, vision, and overall plan for ERM
- Establishing an ERM framework, including a risk taxonomy

Stage 2: Early Development (Yellow Belt)

In Stage 2 the ERM program is in the early stages of development. Key objectives during this stage include formalizing roles and responsibilities in an ERM policy, identifying key risks through risk assessments, and providing risk education to enhance risk knowledge and awareness. Stage 2 may take 1-2 years and typical activities include:

- Establishing an ERM policy, including roles and responsibilities
- Performing annual risk assessments across business units
- Coordinating risk identification and control processes across risk, audit, and compliance functions
- Providing risk education for the board of directors, as well as risk training for a wider group of employees
- Establishing risk functions across the business units

Stage 3: Standard Practice (Green Belt)

In Stage 3 the organization is establishing more frequent and granular risk analyses. Key objectives during this stage include performing more frequent risk assessments, and developing risk quantification processes. This stage may take 1-3 years and activities may include:

- Updating risk assessments on a quarterly or monthly basis
- Developing risk databases, including loss-event information
- Developing KRIs and reporting on enterprise-wide risks on a monthly basis
- Integrating credit risk and market risk models, and building operational risk models
- Developing risk-adjusted performance measurement methodologies

Stage 4: Business Integration (Brown Belt)

In Stage 4 the focus is to integrate ERM into business management and operational processes. ERM tools and practices become more distributed throughout the organization. It is during this stage that risk and return tradeoffs in business decisions are evaluated more explicitly. Key objectives include quantifying the "cost of risk" to support pricing and risk transfer decisions, assessing business risks upfront as part of business and product development, developing automated risk reporting and escalation technologies, and linking risk and compensation. Stage 4 may take 2-4 years and include the following:

- Expanding the scope of ERM to include business risk
- Allocating economic capital to underlying market, credit, operational, and business risks
- Incorporating the cost of risk into product and relationship pricing, as well as portfolio management and risk transfer strategies
- Integrating risk reviews into new business and product approval processes
- Automating ERM reporting through the use of electronic dashboards, including customized queries and real-time escalations
- Establishing "trigger points" to make timely business decisions, including risk mitigation and exit strategies
- Developing feedback loops on risk management performance
- Linking risk management performance and executive compensation

Stage 5: Business Optimization (Black Belt)

In the most advanced stage, ERM is applied to optimize business performance and enhance relationships with key stakeholders. Key objectives in Stage 5 include integrating ERM into strategy development and execution, maximizing firm value by optimizing risk-adjusted profitability, providing risk transparency to key stakeholders, and helping customers manage their risks. Stage 5 is an ongoing process and may include the following activities:

- Expanding the scope of ERM to include strategic risk
- Integrating ERM into strategic planning processes
- Maximizing firm value by actively allocating organizational resources at the "efficient frontier"
- Providing risk transparency to key stakeholders – regulators, investors, rating agencies – with respect to current risk exposures and future risk drivers
- Leveraging risk management skills, tools, and information to deepen customer relationships by helping them manage their risks