CHAPTER 1

Fundamental Concepts and Current State

INTRODUCTION

In October 1517, Ferdinand Magellan requested an investment of 8,751,125 silver maravedis from Charles I, King of Spain. His goal: to discover a westerly route to Asia, thereby permitting circumnavigation of the globe. The undertaking was extremely risky. As it turned out, only about 8 percent of the crew and just one of his four ships completed the voyage around the world. Magellan himself would die in the Philippines without reaching home.

What would motivate someone to undertake this kind of risk? After all, Magellan stood to gain only if he succeeded. But those long-term rewards, both tangible and intangible, were substantial: not only a percentage of the expedition's revenues, but also a 10-year monopoly of the discovered route, and numerous benefits extending from discovered lands and future voyages. What's more, he'd earn great favor with a future Holy Roman Emperor, not to mention fame and the personal satisfaction of exploration and discovery.

But I doubt that even all of these upsides put together would have convinced Magellan to embark on the voyage if he knew that it would cost him his life. As risky as the journey was, most risks that could arise likely appeared manageable. Magellan already had a great deal of naval experience and had previously traveled to the East Indies. He raised sufficient funding and availed himself of the best geographic information of the day.[1]

All in all, Magellan's preparations led him to the reasonable expectation that he would survive the journey to live in fame and luxury. In other words, by limiting his downside risk, Magellan increased the likelihood that he would reap considerable rewards and concluded that the rewards were worth the risk.

Whether taking out a loan or driving a car, we all evaluate risk in a similar way: by weighing the potential upsides and trying to limit the downsides. Like Magellan, anyone evaluating risk today is taking stock of what could happen if things don't go as planned. Risk measures the implications of those potential outcomes. In our daily lives, risk can cause deviation from our expected outcome and keep us from accomplishing our goals. Risk can also create upside potential. We will use a similar definition to define risk in business.

The purpose of this book is to provide the processes and tools to help companies optimize their risk profiles, but first we must have the necessary vocabulary for discussing risk itself. Then we can begin to construct a working model of an enterprise risk management (ERM) program, which we will flesh out over the course of this book. This chapter will cover the fundamental concepts and summarize ERM's history and current state of the art.

But first, some definitions.

WHAT IS RISK?

Risk can mean different things to different people. The word evokes elements of chance, uncertainty, threat, danger, and hazard. These connotations include the possibility of loss, injury, or some other negative event. Given those negative consequences, it would be natural to assume that one should simply minimize risks or avoid them altogether. In fact, risk managers have applied this negative definition for many years. Risk was simply a barrier to business objectives, and the object of risk management was to limit it. For this reason, risk models were designed to quantify expected loss, unexpected loss, and worst-case scenarios.

In a business context, however, risk has an upside as well as a downside. Without risk there would be no opportunity for return. A proper definition of risk, then, should recognize both its cause (a variable or uncertain factor) and its effect (positive and negative deviation from an expected outcome). Taken thus, I define risk as follows:

> *Risk is a variable that can cause deviation from an expected outcome, and as such may affect the achievement of business objectives and the performance of the overall organization.*

To understand this definition more fully, we need to clarify seven key fundamental concepts. It is important not to confuse any of these with risk itself, but to understand how they influence a company's overall risk profile:

1. Exposure
2. Volatility

3. Probability
4. Severity
5. Time Horizon
6. Correlation
7. Capital

Exposure

Risk exposure is the maximum amount of economic damage resulting from an event. This damage can take the form of financial and/or reputational loss. All other factors being equal, the risk associated with that event will increase as the exposure increases. For example, a lender is exposed to the risk that a borrower will default. The more it lends to that borrower, the more exposed it is and the riskier its position is with respect to that borrower. Exposure measurement is a hard science for some risks—those which result in direct financial loss such as credit and market risk—but is more qualitative for others, such as operational and compliance risk. No matter how it is measured, exposure is an evaluation of the worst–case scenario. Magellan's exposure consisted of the entire equity invested by King Charles I, his own life, and the lives of his crew.

Volatility

Volatility is a measure of uncertainty, the variability in potential outcomes. More specifically, volatility is the magnitude of the upside or downside of the risk taken. It serves as a good proxy for risk in many applications, particularly those dependent on market factors such as options pricing. In other applications it is an important driver of the overall risk in terms of potential loss or gain. Generally, the greater the volatility, the greater the risk. For example, the number of loans that turn bad is proportionately higher, on average, in the credit card business than in commercial real estate. Nonetheless, real estate lending is widely considered to be riskier, because the loss rate is much more volatile. Lenders can estimate potential losses in the credit card business (and prepare for them) with greater certainty than they can in commercial real estate. Like exposure, volatility has a specific, quantifiable meaning in some applications. In market risk, for example, it is synonymous with the standard deviation of returns and can be estimated in a number of ways. The general concept of uncertain outcomes is useful in considering other types of risk as well: A spike in energy prices might increase a company's input prices, for example, or an increase in the turnover rate of computer programmers might negatively affect a company's technology initiatives.

Probability

The more likely an event—in other words, the greater its probability—the greater the risk it presents. Events such as interest rate movements or credit card defaults are so likely that companies need to plan for them as a matter of course. Mitigation strategies should be an integral part of the business's ongoing operations. Take the case of a modern data center. Among potential risks are cyberattack and fire, with the probability of the latter considerably lower than that of the former. Yet should the data center catch fire, the results would be devastating. Imagine that the company maintains backup data as part of its cybersecurity program. Simply housing that data in a separate, geographically remote facility would address both risks at a cost only incrementally greater than addressing just one. As a result, the company can prepare for the highly unlikely but potentially ruinous event of fire.

Severity

Whereas exposure is defined in terms of the worst that could *possibly* happen, severity, by contrast, is the amount of damage that is *likely* to be suffered. The greater the severity, the greater the risk. Severity is the partner to probability: If we know how likely an event is to happen, and how much we are likely to suffer as a consequence, we have a pretty good idea of the risk we are running. Severity is used to describe a specific turn of events, whereas exposure is a constant which governs an entire risk scenario. Severity is often a function of other risk factors, such as volatility in market risk. For example, consider a $100 equity position. The exposure is $100, since the stock price could theoretically drop all the way to zero and the whole investment could be lost. In reality, however, it is not likely to fall that far, so the severity is less than $100. The more volatile the stock, the more likely it is to fall a long way—so the severity is greater and the position riskier. In terms of a credit risk example, the probability of default is driven by the creditworthiness of the borrower, whereas loss severity (i.e., loss in the event of default) is driven by collateral, if any, as well as the order of debt payment.

Time Horizon

Time horizon refers to the duration of risk exposure or how long it would take to reverse the effects of a decision or event. The longer an exposure's duration, the greater its risk. For example, extending a one-year loan is less risky than extending a 10-year loan to the same borrower. By the same token, highly liquid instruments such as U.S. Treasury bonds are generally less risky than lightly traded securities such as unlisted equity, structured

derivatives, or real estate. This is because investors can shed their positions in liquid vehicles quickly should the need arise while illiquid investments would take longer to sell, thus increasing time horizon—and risk. When it comes to operational risk, time horizon often depends on a company's level of preparation. A fire that burns a computer center to the ground will leave a company exposed until backup facilities come online, so the risk is greater for organizations that do not have well-established and tested procedures in place. Monitoring, preparation, and rapid response are key. With cybersecurity, preventing all attacks is an unrealistic expectation, but malware detection ("dwell time") and risk mitigation ("response time") are critical drivers of potential damage. Problems arise when companies do not recognize that a risk event has occurred, thus lengthening the time horizon associated with that risk, or if they have not developed a proper risk mitigation strategy.

Correlation

Correlation refers to how risks in a business are related to one another. If two risks behave similarly—that is, they increase for the same reasons or by the same amount—they are considered highly correlated. The greater the correlation, the greater the risk. Correlation is a key concept in risk diversification. Highly correlated risk exposures increase the level of risk concentrations within a business. Examples include loans to a particular industry, investments in the same asset class, or operations within the same building. Risk diversification in a business is inversely related to the level of correlations within that business. Financial risks can be diversified through risk limits and portfolio allocation targets, which cap risk concentrations. Operational risk can be diversified through separation of business units or through the use of redundant systems. A key objective in operational risk management is to reduce "single points of failure," or SPOFs.

A word of caution, however: Seasoned risk professionals recognize that price correlations approach one during times of crisis. For example, during the 2008 financial crisis, all global asset prices (e.g., real estate, equities, bonds, and commodities) fell in concert, with the exception of U.S. Treasuries. For this reason, companies should stress-test their correlation assumptions, as diversification benefits may evaporate just when they are most needed.

Capital

Companies hold capital for two primary reasons: The first is to meet cash requirements such as investments and expenses, and the second is to cover unexpected losses arising from risk exposures. The level of capital that management wants to set aside for these two purposes is often called *economic*

capital. The overall level of economic capital required by a company will depend on the credit rating it wants. A credit rating is an estimate of how likely a company is to fail. It is less likely to fail if it has more capital to absorb any unexpected loss. The more creditworthy it wants to be, the more capital it will have to hold against a given level of risk. The allocation of economic capital to business units has two important business benefits: It links risk and return and it allows the profitability of all business units to be compared on a consistent risk-adjusted basis. As a result, business activities that contribute to, or detract from, shareholder value can be identified easily so management has a powerful and objective tool to allocate economic capital to its most efficient uses.

In addition to economic capital, risk managers should consider human capital (management talent, experience, and track record) and liquidity reserves relative to a company's risk profile. The combination of economic capital, human capital, and liquidity reserves represents the "risk capacity" of the company.

WHAT DOES RISK LOOK LIKE?

The above concepts interact to determine the specific risk levels and enterprise risk profile of an organization. For individual risks—such as credit, market, and operational—the risk levels are greater the higher the exposures, probabilities, severities, and time horizons of the specific positions. At the portfolio level, the risk profile will be greater the higher the concentrations and correlations *within* that portfolio of risks. At the overall level, the correlations *across* risk portfolios (e.g., credit risk, market risk, operational risk, etc.), and the organization's risk capacity, will determine the enterprise risk profile.

Risk Is a Bell Curve

A simple visualization effectively synthesizes these ideas: a bell curve. The notion that *risk is a bell curve* is a key idea that I will discuss throughout the book. When using bell curves to represent risk in a given context, each point on the curve represents a different possible outcome. The horizontal axis provides the range of outcomes, and the vertical axis provides the probabilities associated with those outcomes. As such, the bell curve is a vector of probabilities and outcomes, and collectively these probabilities and outcomes represent the aggregate risk profile. Figure 1.1 provides an illustration of a bell curve.

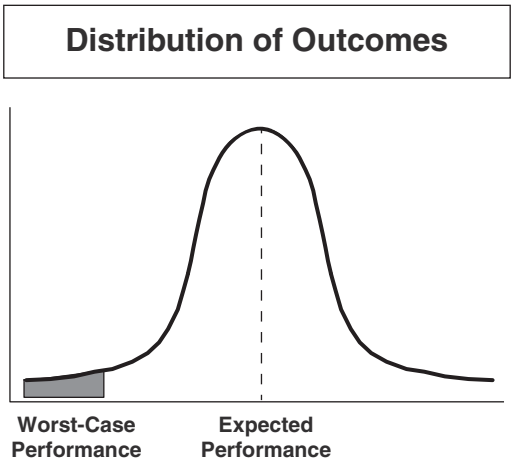

FIGURE 1.1 Risk as a Bell Curve

It is important to consider the following points when conceptualizing and quantifying risk as a bell curve:

- ***Risk comes in different shapes and sizes.*** Some risks—such as interest rate risk or market risk—tend to be symmetrical.[2] These risks are normally distributed where there is equal probability of gains or losses of similar sizes. Other risks—such as credit risk or operational risk—are asymmetrical with more downside than upside. If a loan pays off, the lender gains a few percentage of interest income, but if it defaults, the lender can lose the entire principal. If a core IT operation is running smoothly, it is business as usual, but a failure can cause significant business disruption. Risks can also be asymmetrical with more upside than downside, such as an investment in a new drug or a disruptive technology. Such investments can produce unlimited upside but the downside is limited to the amount of the investment.
- ***Risk should be measured relative to business objectives.*** The risk metric used should be based on the context of the specific business objective and desired performance. For example, at the enterprise level the risk metrics can be earnings, value, and cash flows to quantify earnings-at-risk (EaR), capital-at-risk (economic capital or CaR), and cash flow-at-risk (CFaR), respectively. Such performance-based models can support the organization in managing corporate-wide objectives related to earnings performance, capital adequacy, and liquidity risk. At the individual

business or risk level, the risk metric used should be linked to the specific business objective, such as sales performance, IT resilience, and talent management.

- ***The bell curve provides the downside, but also the mean and upside.*** Risk managers tend to focus mainly on downside risk. For example, EaR, economic capital, and CFaR models usually quantify the downside outcome at a 95–99% confidence level. However, a proper definition of risk must include all eventualities. The bell curve provides the full spectrum of risk, including the mean (i.e., expected outcome) as well as the downside and upside scenarios. By adopting a more expansive consideration of potential outcomes, risk managers can make more informed risk-based business decisions. The same variables that can produce unexpected loss can also produce unexpected gain. Downside risk analysis can inform capital management, hedging, insurance, and contingency planning decisions. Analyses of expected value can support financial planning, pricing, and budgeting decisions while upside risk analysis can shape strategic planning and investment decisions.
- ***The objective of management is to optimize the shape of the bell curve.*** It has often been said that value maximization is the objective of management. To accomplish this objective, management must maximize the risk-adjusted return of the company. In other words, it must optimize the shape of the bell curve. For example, management should establish risk appetite statements and risk transfer strategies to control downside tail risks. Pricing strategies should fully incorporate the cost of production and delivery, as well expected loss and economic capital cost. Strategic planning and implementation should increase expected earnings and intrinsic value (moving the mean of the bell curve to the right). This objective extends to a non-profit organization, but return is driven by its organizational mandate.

By conceptualizing—and ideally, quantifying—any risk as a bell curve, companies can manage them most effectively. This applies even to intangible risks that are difficult to quantify. Let's use reputational risk as an example. The mean of the bell curve represents the current reputational value of the organization. Reputational risks would include the key variables and drivers for the organization in meeting the expectations of its main stakeholders: customers, employees, regulators, equity holders, debt holders, business partners, and the general public. As with other risks, these variables and drivers can be measured and managed to enhance the organization's reputation, including downside and upside risk management.

ENTERPRISE RISK MANAGEMENT (ERM)

The concepts I've described so far form the foundation for risk analysis, but understanding risk is just a preliminary step toward managing it. We are now ready to lay the groundwork for implementing enterprise risk management (ERM). Specifically, we will discuss:

- A definition of ERM
- Early development of risk management
- The development of ERM in the 1990s

This brief overview of ERM will show how the events of the past half-century have shaped ERM's current critical role in business strategy.

What Is Enterprise Risk Management?

A proper definition of ERM should describe what it is, how it works, its main objective, and its main components. With these criteria in mind, I will define ERM as follows:

> *ERM is an integrated and continuous process for managing enterprise-wide risks—including strategic, financial, operational, compliance, and reputational risks—in order to minimize unexpected performance variance and maximize intrinsic firm value. This process empowers the board and management to make more informed risk/return decisions by addressing fundamental requirements with respect to governance and policy (including risk appetite), risk analytics, risk management, and monitoring and reporting.*

Let's briefly expand on this definition. First, ERM is a management process based on an integrated and continuous approach, including understanding the interdependencies across risks and implementing integrated strategies. Second, the goal of ERM is to minimize unexpected performance variance (defensive applications) and to maximize intrinsic firm value (offensive applications). As discussed, risk management is not about minimizing or avoiding risks, but optimizing risk/return trade-offs (the bell curve). Third, an ERM program supports better decisions at the board and management levels. Board decisions may include establishing risk appetite, capital and dividend policy, as well as making strategic investments.

Management decisions may include capital and resource allocation, customer and product management, pricing, and risk transfer. Finally, the key components of ERM include governance and policy (including risk appetite), risk analytics, risk management, and monitoring and reporting. These four components provide a balanced and integrated framework for ERM.

Early Development of Risk Management

Protecting ourselves against risk is a natural practice that goes back well before Magellan. In fact, one could argue that risk management has existed as long as human history. As long as attacks from animals, people, or businesses have been a threat, we have constructed safeguards and defenses. As long as buildings have faced floods and fires, risk management has included structural design and materials used, or, in modern times, transferring that risk to an insurer. As long as money has been lent, lenders have diversified among borrowers and discriminated between high- and low-risk loans. Despite the intuitive nature of risk management—or perhaps because of it—it did not become part of formal business practice until the second half of the last century.

It wasn't until 1963 that the first discussion on risk appeared in an attempt to codify and improve such practices. In their *Risk Management and the Business Enterprise,* authors Robert Mehr and Bob Hedges posited a more inclusive risk-management practice that went beyond the status quo of merely insuring against risk. They proposed a five-step process reminiscent of the scientific method: Identify loss exposures, measure those exposures, evaluate possible responses, choose one, and monitor the results. They also described three general approaches to handling risks: risk assumption, risk transfer, and risk reduction. At this early stage, risk management emphasized hazard risk management. Financial risk entered the scene later. These traditional theories focused on what are called "pure" risks, such as natural disasters, which result either in a loss or no change at all, but never an improvement. Modern ERM practice now encompasses speculative risk, which involves either loss or gain. Stock market investment is a classic example of speculative risk.

The lack of attention to financial risk in early risk management programs reflected the comparative stability of global markets at the time. This began to change in the following decade. In 1971, the United States abandoned the gold standard, and in 1972, many developed countries withdrew from the 1944 Bretton Woods agreement, which had kept most foreign exchange rates within narrow bands since World War II. This brought an unprecedented volatility to global exchange rates. The Seventies also brought soaring oil prices due to the decision by the Organization of Petroleum Exporting Countries (OPEC) to decrease global supply after the 1973 Yom Kippur

War. Like the proverbial butterfly's wings, this had multiple effects around the globe. Rising oil prices drove up inflation, which caused the U.S. Federal Reserve to raise interest rates to historical levels, a response that fueled volatility not only in the United States but worldwide as well. These economic changes created a need for financial risk management that companies had not experienced before.

The Seventies and early Eighties saw the introduction of new financial risk-management tools, particularly derivatives such financial futures, options, and swaps. These new tools allowed companies to manage volatile interest rates and foreign exchange rates and were effective when used properly. But some firms suffered severe losses from ill-conceived derivatives trades. In 1993, the German corporation Metallgesellschaft barely avoided bankruptcy after a $1.3 billion loss due to oil futures contracts. The next year, Procter & Gamble lost $157 million due to an injudicious swap. In the Nineties, devastating losses due to operational risk were all too common, often for lack of standard controls such as management supervision, segregation of duties, or basic checks and balances. In 1995 Barings Bank was driven bankrupt after a loss of $1.3 billion due to unauthorized derivatives trades. Only months later, Daiwa Bank was forced to end all U.S. operations in the aftermath of a $1.1 billion scandal surrounding unauthorized derivatives trading. Early risk managers operating under traditional practices simply overlooked operational risk, leaving it to the relevant business units.[3]

THE CASE FOR ERM

Despite the high-profile losses, the 1990s saw important steps forward in ERM. Risk quantification became more sophisticated with the advent of value-at-risk models (VaR). Before VaR, the primary risk measure was probable maximum loss, which is similar to the potential loss and can be expressed in the question, "What's the worst that could (reasonably) happen?" By contrast, a VaR metric predicts, to a specific level of confidence, potential losses over various time intervals. Early versions of modern ERM appeared around this time as companies developed more sophisticated risk quantification methods for market risk and credit risk, as well as initial operational risk management programs. In the mid-1990s, companies began appointing chief risk officers (CROs) to establish a C-suite executive who could integrate the various risk management functions under a single organization. Steady progress continued until the 2008 financial crisis, which revealed numerous shortcomings in risk management models and reminded businesses of the need for improvement.

Organizations continue to discover the value of ERM and work to implement their own customized programs. Let us look at three perspectives:

- The current demand for ERM
- The current state of ERM
- What ERM can look like and what it can do

The Current Demand for ERM

We work in a business climate rife with volatility and risk. A recent survey by the Association for Financial Professionals (AFP) found that 59 percent of financial professionals consider their firms to be subject to more earnings uncertainty now than five years previously. Only 12 percent believe they are operating with more certainty today.[4] A similar majority said it is more difficult to forecast risk than it was five years ago and foresaw it getting even more difficult three years hence. Risks considered to have the greatest impact on earnings were (in order of decreasing frequency): customer satisfaction and retention, regulatory risk, GDP growth, political risk, energy price volatility, labor and HR issues, and natural disasters.

So what are firms doing to prepare for these risks? By their own admission, less than they would like. Only 43 percent of respondents to the AFP study felt their ability to forecast crucial variables was relatively strong while the rest needed improvement; 10 percent even considered their capabilities weak to nonexistent. Companies recognize a growing need for changes in risk management processes. Organizations are hiring risk professionals, investing in IT systems, automating financial processes, and placing a greater focus on risk awareness and culture. Many have beefed up executive review of business strategy and assumptions (63 percent) while others have increased risk analysis and forecasting as well as reports to management.

The individual ultimately responsible for managing this growing risk is frequently the CFO, named by 38 percent of the firms surveyed. Another 28 percent named the CEO or COO; 14 percent operated under a risk committee, 11 percent named the treasurer, and only 9 percent had a chief risk officer (CRO) as the primary overseer of risk management. It is important to note that these results were based on a cross-industry survey.

Old Methods Won't Work

Today, companies recognize the need for better risk management, but amplifying old methods or tweaking existing structures to deal with increased risk carries dangers. Just one example: the highly interdependent

risks that organizations frequently face. Figure 1.2 provides an illustration of risk interdependency in the form of a Venn diagram.

Key interdependencies exist between financial and business risk, business and operational risk, and operational and financial risk. Furthermore, each major risk category comprises subcategories. For example, financial risk, as demonstrated in the figure, can be broken down into market risk, credit risk, and liquidity risk. These financial risks in turn have their own interdependencies.

Let's examine loan documentation as a practical example of a key interdependency between operational risk and financial risk (in particular credit risk). As a business process, loan documentation quality is considered an operational risk. If a loan is performing (i.e., the borrower is making timely interest and loan payments), the quality of that specific loan document has no real economic impact. But if the loan is in default, the documentation quality can have a significant impact on loss severity because it affects collateral and bankruptcy rights. Loss analyses conducted by James Lam & Associates at lending institutions revealed that up to one-third of "credit losses" were associated with operational risks.

According to the AFP survey above, about 12 percent of firms still use a siloed, decentralized structure. But in a complex, interlocking system of company-wide risks, this strategy is clearly insufficient. Some risks may remain poorly understood or even ignored. Gaps and redundancies may go unnoticed and unaddressed. And aggregate risk exposures across the organization could pose hidden threats. For example, if business units use different methodologies and systems to track counterparty risk, then it is difficult to quantify the aggregate exposure for a single counterparty. While the individual exposures at each business unit might be acceptable, the total counterparty exposure for the organization may exceed tolerance levels.

On the other hand, an overly centralized system of risk management can fail to integrate the relevant risk information into the decision-making processes of an organization. A full 28 percent of organizations have a centralized risk management system, which can lead to ineffectual top-down management of risk-related decisions. Most organizations (60 percent) operate under a structure with centralized processes but decentralized implementation. In this arrangement, the risk monitoring, reporting, and systems are centralized, but the implementation of risk management strategies is in the hands of each business unit.[5]

In a volatile economic climate, the most successful companies establish comprehensive, fully integrated risk management processes at each level of decision-making. ERM provides integrated analyses, strategies, and reporting with respect to an organization's key risks, which address their interdependencies and aggregate exposures. In addition, an integrated ERM

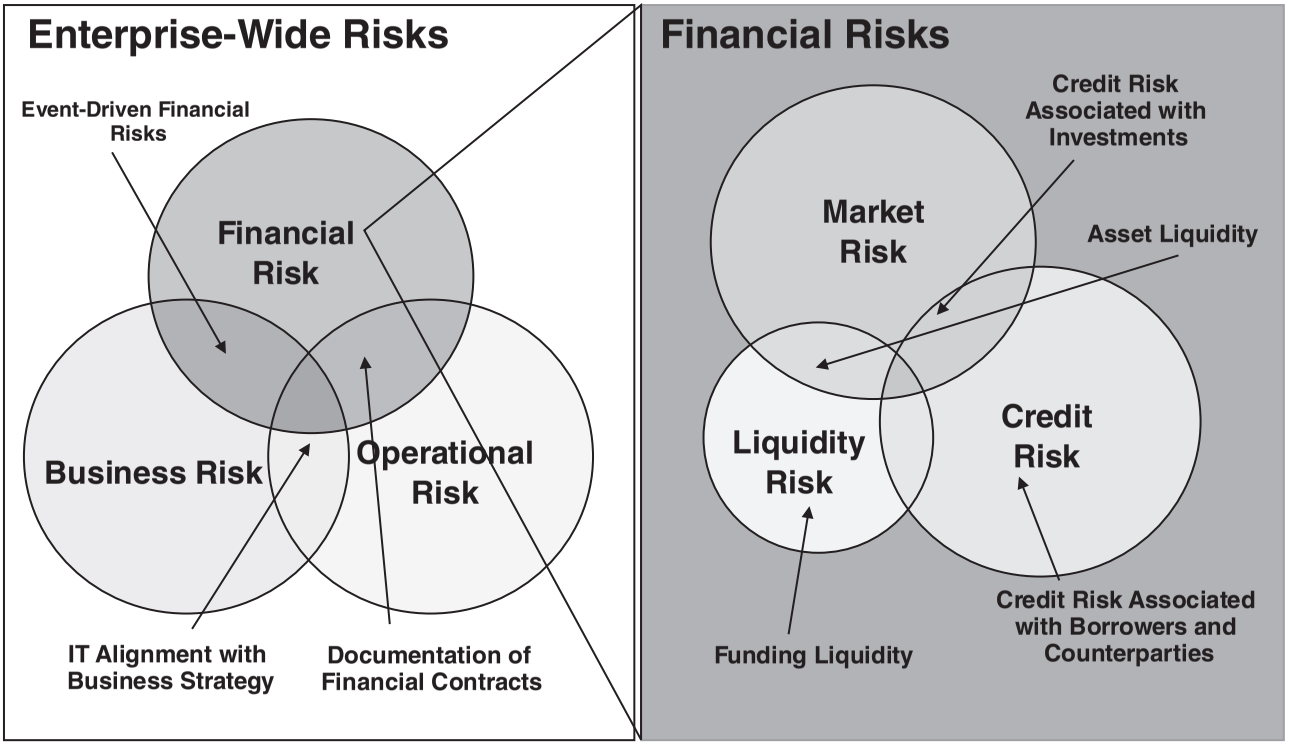

FIGURE 1.2 Risk Interdependencies

framework supports the alignment of oversight functions such as risk, audit, and compliance, which rationalizes risk assessment, risk mitigation, and reporting activities. It also considers how macroeconomic factors, such as interest rates, energy prices, economic growth, inflation, and unemployment rate, can impact the organization's risk/return profile. This interweaving of ERM into an organization adds strength throughout, whereas merely applying a superstructure from the top down may leave weaknesses unaddressed.

Integration Adds Value

The value that integration adds is visible in many areas of business and life, including fitness and sports. Over the past few decades, many disciplines have experienced greater effectiveness through integration. Take the example of cross-training in fitness. By integrating cardiovascular workouts with strength training, flexibility, and endurance, athletes can prevent and rehabilitate injuries as well as enhance strength and power. Similarly, the integration of various fighting styles into mixed martial arts (MMA) has added value to centuries-old practices and beliefs. Whereas martial artists once argued about which style was superior, the emergence of MMA has changed their attitude. Mixed martial artists combine karate, kung fu, jujitsu, tae kwon do, wrestling, and multiple other fighting styles, allowing them to adapt to any situation. This gives them a significant advantage over a fighter trained in a single style.

So too, integration of ERM into business strategy leads to more informed and effective decisions. In fact, I believe the integration of strategy and risk is the next frontier in ERM, as it allows a company's board and management to understand and challenge the underlying assumptions and risks associated with their business strategy. Expanding technological capabilities have put this within the grasp of most companies. System integration allows for enterprise-level data management, robust business and data analytics, straight-through transaction processing, and more effective reporting and information sharing.

According to a 2013 Deloitte study, 81 percent of the executives surveyed now have an explicit focus on managing strategic risks, in contrast to the traditional focus on financial, operational, and regulatory ones.[6] The study suggests a reason, too: Strategic risks represented approximately 36 percent of the root causes when publicly traded companies suffered significant market value declines over the past 10 years. This was followed by external risks (36 percent), financial risks (17 percent), and operational risk (approximately 10 percent).[7]

WHERE ERM IS NOW

The numbers show that corporations around the world are recognizing risk management as a priority and moving toward integrated ERM. The 2013 Deloitte Global Risk Management survey indicated that 83 percent of all global financial institutions have an ERM program or are in the process of implementing one, up from 59 percent in 2010.

As a management framework, ERM has been more widely adopted than other management frameworks (e.g., reengineering, balanced scorecard, total quality management). Organizations with established ERM programs have realized and reported significant benefits. For example, 85 percent of financial institutions that had ERM programs in place reported that the total value derived from their programs exceeded costs.[8] Three quarters of today's executives feel that their ERM programs provide significant value compared with merely half in 2008.

As ERM adoption has increased over the past several years, the CRO has grown in stature. The 2013 Deloitte Global Risk Management survey indicated that 89 percent of global financial institutions had a CRO or equivalent position. Moreover, 80 percent of the institutions said their CRO reports directly to the CEO and had a formal reporting relationship with their board, up from about 53 percent in 2010.

Outside the financial sector, it's a different story, however. A 2012 paper produced by McKinsey & Company[9] pointed out that, unlike financial institutions, most corporates still do not have a CRO, leaving the de facto role of risk manager to the CFO. Furthermore, the goals for ERM improvement vary between the two sectors. Financial institutions are keen to improve their risk culture, IT, and data infrastructure while corporates focus on improving risk-related decisions and processes. Still, the frequency and heft of the CRO is growing throughout all sectors.

Board involvement in ERM has increased as well, particularly since the global financial crisis. Several surveys indicate that risk management has replaced accounting issues as the top concern for corporate boards. Approximately 80 percent of boards now review risk policies and risk appetite statements.[10]

Although ERM has made significant progress over the past decade, much remains to be done. In a sense, the global financial crisis was the ultimate risk management "stress test." Many organizations failed, and even those with established ERM programs reported mixed results. Today, organizations appear to understand the need for change. Deloitte's 2013 survey reported that 94 percent of organizations have changed their

approach to strategic risk management over the previous three years. Companies cite cultural issues and integrating data across the organization as the two biggest stumbling blocks to improvement.[11]

WHERE ERM IS HEADED

With ERM's role increasing within organizations and across industries, the roles of the board and upper management have to adapt. Certainly, the CRO bears the brunt of this change, but the CEO, CFO, and board of directors all find that ERM is taking a more prominent position in their priorities. Here's how these parties will increasingly work together as ERM becomes embedded in corporate culture.

The CRO carries the central responsibility of ensuring that each gear in the ERM process is meshed and moving properly. He or she develops the risk appetite statement (RAS) in collaboration with the CEO and the CFO to ensure that it complies with regulations, current markets, and the organization's business strategy and objectives. The CRO monitors the risk climate, ensures compliance with regulations, sees that the firm operates within its risk appetite, and keeps the CEO and the board of directors well informed through established reporting processes.[12]

The CEO in turn sets "the tone from the top" in words and actions. He or she sets the appropriate business and risk management objectives, holds organizational leaders accountable for their decisions and actions, and ensures that a strong risk culture is in place. The CFO is responsible for incorporating the RAS into financial decision making, including investment, funding, and hedging strategies. If risk exposures exceed the RAS, the CFO, along with the CRO, must take mitigating action and bring it to the attention of the CEO and board.

Finally, the board of directors provides risk governance, independent oversight, and credible challenge. It reviews the RAS for compatibility with the organization's goals, approves it, and holds senior management accountable for its implementation. The board monitors the business plans against the RAS to check if they are aligned. The board also provides oversight of key business, regulatory, and reputational risk issues, as well as monitors the organization's ERM effectiveness and risk culture.

As we've seen, ERM is providing value for a large number of corporations despite its current challenges. But it is my view that we're really just beginning to see how much value ERM can offer. In less than a decade, risk management has risen to the top of corporate agendas for senior

management and the board across all industry sectors. What form are these efforts taking? This question will be the focus of the next chapter, in which we'll take a deeper look at the economic, financial, and cultural drivers that are changing the face of enterprise risk management.

NOTES

1. Findlay, James. "Marvellous Countries and Lands," Bienes Center, 2002.
2. Certain factors such as the prepayment option in mortgage loans and securities can create negative convexity, or a disadvantaged, asymmetrical interest rate risk profile for the mortgage lender or investor. For example, when rates rise and mortgage prepayment speeds decrease, the longer duration will produce a greater value loss. Conversely, when rates drop and mortgage prepayment speeds increase, the shorter duration will produce a smaller value gain.
3. D'Arcy, Stephen P. and Brogan, John C. "Enterprise risk management," *Journal of Risk Management of Korea*, 12, 2001. http://www.casact.org/.
4. Wittenberg, Alex. *2013 AFP Risk Survey*, Association for Financial Professionals, 2013.
5. Wittenberg, Alex. *2013 AFP Risk Survey*.
6. Global Risk Management Survey, Eighth Edition: "Setting a Higher Bar," Deloitte Touche Tohmatsu Limited, 2013.
7. Kambil, Ajit. "The Value Killers Revisited: A Risk Management Study," Deloitte LLP, 2014.
8. Global Risk Management Survey, Seventh Edition: "Navigating in a Changed World," Deloitte Touche Tohmatsu Limited, 2011.
9. Pergler, Martin. *Enterprise Risk Management*, McKinsey &Company, 2012.
10. GRM Survey, Eighth Edition, Deloitte.
11. *Exploring Strategic Risk: A Global Survey*, Deloitte Touche Tohmatsu Limited, 2013.
12. "Principles for an Effective Risk Appetite Framework," Financial Stability Board, 2013.