PART ONE

Basic ERM Infrastructure

CHAPTER ONE

1 Introduction

History is the sum total of the things that could have been avoided.

Konrad Adenauer

ENTERPRISE RISK MANAGEMENT, or ERM, is generally defined as follows:

> The process by which companies identify, measure, manage, and disclose all key risks to increase value to stakeholders.

One of the challenges with ERM lies in understanding what this definition means. There are many interpretations, and some would say misinterpretations, of this short definition. In the next chapter, we will fully and properly define ERM. For now, consider ERM simply as an approach to treat risk holistically in an organization.

EVOLUTION OF ERM

ERM has been gaining significant momentum in recent years. We will discuss the following eight most important factors driving this trend, which are as follows:

1. Basel Accords
2. September 11th
3. Corporate accounting fraud
4. Hurricane Katrina
5. Rating agency scrutiny
6. Financial crisis
7. Rare events
8. Long-term trends

The first seven factors involve significant discrete events and are listed in chronological order, while the remaining factor includes trends that have developed gradually over time. Some of the discrete events originate from, or relate primarily to, the financial services sector. However, it is helpful for those in all sectors to understand these events because they are commonly known in ERM circles and their impacts on ERM are felt in all industry sectors. In addition, it is helpful to understand the chronology because the order of events has played a role in ERM development. The cumulative impact of events, and the regulatory and corporate responses to them, has led to the current environment for ERM.

BASEL ACCORDS

Basel II,[1] an international guideline for risk management, influenced the advancement of ERM practices in the financial services sector. The Basel Accords are guidelines developed by a group of global banking regulators in an attempt to improve risk management practices. Basel II, the second of two accords developed by the Basel Committee on Banking Supervision, was published in 2001.

There are three pillars in Basel II:

- Pillar 1: Minimum capital requirements
- Pillar 2: Supervisory review
- Pillar 3: Market discipline

Pillar 1 specifies methods to calculate capital requirements, offering standardized options based on industry averages and advanced options for more sophisticated banks based on their own internal models, customized to account for the specifics of the company, its businesses, and its risks, and largely using management's own estimates for most parameters.

Pillar 2 allows for supervisors to review the bank's risk management practices and risk exposures and, if necessary, apply a multiplier to increase the amount of minimum required capital calculated in Pillar 1.

Pillar 3 addresses appropriate risk disclosures.

The most important advancement since Basel I was the expansion of scope to include operational risks, moving banks in the direction of a holistic treatment of risk (although many other risks, including all strategic risks, are still excluded).

In retrospect, it is easy to criticize and say that the Basel Committee failed in their goal, as evidenced by the global financial crisis that began in the United States in 2007. However, these accords were widely adopted and did represent an improvement from prior practices. Even if the Basel Accords fell short of their goal to develop a standard benchmark for stellar risk management practices, they did however result in an enhanced focus on risk in the banking sector and beyond, as others held up the banking sector as a model for managing risk. Solvency II, a set of risk management standards for European Union (EU) insurance companies scheduled to take effect in November 2012, is clearly influenced by Basel II, and is largely analogous to it.

SEPTEMBER 11TH

The terrorist attacks on the United States on September 11, 2001, advanced our thinking in the area of ERM by raising awareness of four major aspects of risk:

1. Terrorism risk
2. Concentration risk
3. Risk complexity
4. Need for an integrated approach

Terrorism Risk

Virtually all organizations are more aware of the possibility of a terrorist attack as a result of September 11th. Many of these organizations, particularly those

operating in or near major cities or potential terrorist targets, have also thought through various terrorism scenarios. They have examined the potential impacts of an attack impacting their physical assets, employees, customers, stakeholders, suppliers, and/or the economies in which they operate. These exercises have led to some preventive mitigation (such as decentralizing offices) as well as enhanced business continuity plans. An additional benefit is the general raising of awareness of the possibility of the previously unthinkable. This is helpful, since ERM requires management to keep an open mind to a more complete range of future scenarios.

Concentration Risk

Even before September 11th, companies were aware of the danger of concentrations of risk. For example, companies try to avoid depending too much on a single large customer or supplier; investing too much of their assets in any one sector; or having too much knowledge, power, or access concentrated with one employee. However, September 11th dramatically changed the way companies, and governments, thought about concentration risk.

The result was a complete rethinking of where and how resources are, or might become, exposed in a concentrated way to terrorism or other types of risk. Where are our most critical employees located? Where do we gather our most critical employees together? Where are the bulk of our invested assets geographically? Are any of our key customers or suppliers or other credit counterparties exposed to significant concentration risk? One manifestation of this was many employers decentralizing their locations out of major landmark buildings and also out of major cities.

Risk Complexity

September 11th raised awareness of the complexity of risk. A complex set of interdependencies, which remains beneath the surface until a significant disruption reveals it, became apparent in the aftermath of the attacks. There were numerous secondary impacts that were unexpected, or at least had not been examined until then.

Though it may appear obvious now, few would have predicted how severely the airline business would be impacted. After all, statistically, even with a moderate increase in terrorism, flying is still far safer than other modes of travel. According to a study by Sivak and Flannigan published in the January–February issue of *American Scientist*, even if a terrorist event equivalent to September 11th occurred every month, flying would still be safer

than driving.[2] However, the human factor is a significant component of risk complexity. It is more difficult to account for fear and other irrational human tendencies, which often direct actions that are counter to our collective best interests. A Cornell University study found that an additional 725 people lost their lives in just the three months following September 11th as a result of a shift from flying to driving.[3]

Another type of risk complexity that was highlighted as a result of September 11th was that while there are mostly downside impacts from a horrible event, there are often upside impacts as well. For example, anyone in the security business can tell you how much opportunities increased after the attacks. In addition, companies providing teleconferencing benefited as well, as business travel decreased dramatically. While this is not a new concept, again, the sheer scale of September 11th increased awareness that in considering a risk scenario, it is important to factor in the potentially offsetting upside impacts as well.

Need for an Integrated Approach

September 11th highlighted the need for an integrated approach to risk management. It moved the U.S. government closer to managing risks on a basis more consistent with ERM principles. The government reorganization in response to September 11th is analogous to the beginnings of an ERM program. They established the Department of Homeland Security, later organized under the ODNI (Office of the Department of National Intelligence), which centralizes efforts regarding most risks facing the country. One of the key recognitions was that the government was in possession of intelligence which should have, or could have, prevented the attacks, but due to a lack of coordination, sharing, and prioritization of information, a disaster occurred. It is the same within companies. Many companies possess excellent information, but fail to realize their potential—both in terms of averting disasters as well as capitalizing on opportunities—due to a lack of integration between separate business segments.

CORPORATE ACCOUNTING FRAUD

In 2001 and 2002, a wave of accounting scandals rocked the business world. Enron, Tyco, and WorldCom were just three of the most prominent examples. These firms suffered dramatic financial collapses and had executives convicted

and sentenced to prison. The names of these executives—Jeff Skilling, Ken Lay, Andrew Fastow, Dennis Kozlowski, and Bernie Ebbers—still send shudders down the spines of executives everywhere, nearly a decade later. In addition, Arthur Andersen, the audit firm for both Enron and WorldCom, went out of business as a result of the scandals. The fallout from all the accounting scandals included two significant events that led many companies to improve their risk management processes.

The first event involved litigation, and increased the accountability of members of the board of directors and, more important, their personal financial liability, in the event of undetected corporate accounting fraud. In a WorldCom lawsuit, a settlement was reported that involved 10 outside directors paying damages out of their personal assets amounting to approximately 20 percent of their net worth, and which were not allowed to be reimbursed by their directors and officers (D&O) liability insurance coverage. An Enron lawsuit settlement involved similar personal payments from directors.

These settlements were significant in that they led to two major trends. First, serving on a board of directors became less attractive due to the increased liability. Many companies saw directors retiring from the board, and found it more difficult to recruit directors. The second, and more important trend for ERM, is that the remaining directors became more diligent about risk, and began asking management what was being done to protect the company against key risks. In many instances where companies have adopted ERM, it was precipitated by pressure on management from a member of the board of directors.

The second event involved legislation and enhanced the risk management practices of companies and their auditors in relation to ensuring the accuracy of external financial reports. In 2002, the U.S. Congress passed the Sarbanes-Oxley Act, also commonly referred to as SOX. Similar legislation was later adopted elsewhere, including Japan (J-SOX), France, Italy, and some other countries. This legislation required companies to establish a highly detailed and expensive process for identifying risks to, and establishing, documenting, and testing the effectiveness of risk controls for, the financial reporting process, and to have company executives formally attest to the accuracy of the financial reports. In an effort to comply with SOX, many companies adopted a modified version of the COSO Internal Control framework developed in the early 1990s.[4]

Though SOX has been widely criticized as onerous and ineffective, it did raise corporate awareness of risk regarding financial reporting accuracy as well as more generally. Many companies used process maps to help identify

vulnerable areas (e.g., regarding the handoffs and access to data) in the reporting process, and some began to expand the use of process maps to identify risks and inefficiencies in other company processes as well. SOX also empowered employees to identify and address some new risks, as well as to raise, and get funding to resolve, some known issues.

HURRICANE KATRINA

The August 2005 hurricane that devastated the city of New Orleans taught us many lessons regarding risk management, but two of them in particular have helped advance ERM practices in a way that is both lasting and significant. These lessons relate to:

- Worst-case scenarios
- Natural disasters

Worst-Case Scenarios

Like September 11th, Hurricane Katrina opened the imagination up to worst-case scenarios, even though they may be remote in likelihood. According to the U.S. Army Corps of Engineers, Hurricane Katrina was a 1-in-396-year event. The lesson here is to put more emphasis on the impact of risk scenarios, rather than on the likelihood. The likelihood may be very small, but it is more a matter of not exposing yourself to anything that can wipe you out completely.

Natural Disasters

Up until relatively modern times, people have been largely exposed to the elements of nature. For example, before Benjamin Franklin invented the lightning rod in 1747, every city faced the very real possibility of entire neighborhoods burning down with each new lightning storm. Each new technological advance over the years has brought with it more power over our environment, as well as a growing sense of invulnerability.

Katrina reminded us of our vulnerability to natural disasters and the fallibility of our best attempts to prevent or mitigate them. This was dramatically underscored in the wake of the powerful hurricane and the ensuing flooding, which showed the most powerful nation in the world unable to stem the virtual loss of a major city to nature. After Katrina, many companies began

to incorporate more natural disaster scenarios in their ERM programs, and that practice continues today.

RATING AGENCY SCRUTINY

In October 2005, rating agency scrutiny of company ERM programs took a great leap forward. Standard & Poor's (S&P) added ERM as an additional distinct ratings category for their credit ratings of insurance companies, globally. Though the other major rating agencies did not follow their approach precisely, they did begin to highlight how they were addressing ERM, in response to questions raised as a result of S&P's move. S&P's ERM review advanced the global practices of ERM in four ways:

1. Rapid advancement
2. Continual evolution
3. Growth beyond requirements
4. Expansion to all sectors

Rapid Advancement

Insurance companies moved, and moved quickly, to begin implementing an ERM program or enhance their existing ERM programs. S&P's move was bold and brilliant from a marketing perspective. As a separate and distinct component of the overall rating, the ERM ''grade'' a company received would be publicly available. As a result, companies were highly motivated to get a good grade. S&P published their ERM ratings criteria in some detail, and companies used this as a guide for enhancing their ERM programs. Companies needed to be prepared in time for their next meeting with S&P, and since implementing ERM has a long lead time, many scrambled to prepare for the S&P ERM review.

Continual Evolution

Insurance companies began to enhance their ERM programs each year. S&P made a strategic decision to raise the bar on the level of sophistication that would be required to maintain the ERM rating, and did so each year since the introduction of its initial ERM review criteria. Once companies achieved the ERM rating they desired, they quickly became even more concerned about the possibility of losing that rating, and what that might signal to bondholders

and shareholders alike. As a result, S&P helped encourage a continual evolution of ERM programs at these companies.

Growth beyond Requirements

Insurance companies began to take ERM programs even further than S&P requirements. Once companies began to develop robust ERM programs, some of them began to tout how their ERM programs afforded them a competitive advantage. Spurred on by a certain level of competition, others began to investigate how they too could use ERM for competitive purposes.

Expansion to All Sectors

Other sectors became, and continue to become, more aware of the need to advance their ERM programs. S&P enjoyed much success with their insurance ERM reviews, not only in terms of their moving the sector forward in ERM sophistication but also in terms of attention. S&P received a phenomenal level of press coverage for their innovative approach. This led to S&P announcing in May 2008 that they would enhance their ERM reviews as part of their credit ratings of non-financial companies. This is an important and much-needed development, because most non-financial sectors have been lagging in risk management practices as compared to the financial services sector. Although the non-financial sector ERM review is not treated as a distinct ratings category like that in the insurance sector, even before its formal incorporation into the ratings process, these companies are becoming more aware of S&P's ERM criteria, and are acknowledging the need to improve their risk management practices.

FINANCIAL CRISIS

The global financial crisis that began in the United States in 2007 has shaken up the status quo in the world of risk management and has opened the door for all companies to look at how to improve their ERM programs. First, the crisis has clearly laid false the claim by the banking sector that they had best-in-class risk management practices. This is important, because others in the financial services sector had been enamored with the banking approach and were of the opinion that all they had to do was mimic it. In Chapter 9 we describe what banks were and were not doing in terms of ERM practices.

In addition to witnessing the fall of the mighty in the banking sector, companies had their own direct experience in the crisis that, if they survived

it (and many did not), served as a wake-up call. During the heart of the crisis, there was a lull in ERM advancement as individuals and companies were just scampering to survive. However, after the worst seemed to be over, companies in all sectors of the economy began to perform assessments of their ERM programs to determine priorities for enhancements. As before, the financial services sector is actively engaged. However, the non-financial services sector is also moving forward, some companies more quickly than others. In particular, Steve Dreyer, who leads S&P's global initiative to incorporate ERM into their credit ratings for non-financial services companies, indicates that ''coming out of the financial crisis, many companies in the consumer products sector enhanced their ERM activities, in part due to their experience with the financial crisis and its impact on their supply chain. Likewise, energy companies exposed to recession-driven low natural gas prices have focused more intently than ever on proactively managing exposure to commodity price movements.''

Another important consequence of the financial crisis is that it is no longer as difficult for those involved in the ERM process to get management to consider worst-case scenarios. Living ''in the tail''—which refers to experiencing what was previously considered so unlikely an event that it would graphically reside in the extreme downside tail-end portion of the distribution curve illustrating the range of possible events—has opened management's imagination of what else can go badly, and how badly it can go.

In addition, it is expected that fallout from the financial crisis in the forms of legislation, regulation, and litigation could have significant positive impacts on the advancement of ERM globally. At the time of the writing of this book, it is too early to determine these impacts. However, there are two consequences that are worth mentioning that have the potential to accelerate adoption of ERM programs:

1. SEC disclosure regulation
2. Dodd-Frank legislation

SEC Disclosure Regulation

In February 2010, the SEC passed a regulation requiring the disclosure of risk governance as well as risky compensation programs. These are both discussed in Chapter 7. Adopting an ERM program would help companies comply with this regulation. The regulation may reveal the presence, or lack, of good risk

governance at companies. In addition, the regulation requires an ability to determine whether the incentive compensation program is risky, and this cannot effectively be done without a proper ERM program in place.

Dodd-Frank Legislation

In July 2010, the Dodd-Frank legislation became effective. Much of the legislation was written to merely empower regulators to design and implement new requirements, which will take awhile to emerge. However, there is one aspect of the bill that has the potential to advance ERM practices. The bill created a new entity, the Financial Stability Oversight Council, and empowered it to make recommendations regarding new risk management requirements for financial institutions.

RARE EVENTS

In 2009, two threats resurfaced related to risk events so rare that they had not been taken seriously in modern times. Although these threats did not result in significant impacts, they played a part in helping management keep an open mind about rare events, which is important in ERM. The two threats were:

1. H1N1 flu pandemic
2. Pirates

H1N1 Flu Pandemic

For many years, scientists have been saying that it is only a matter of when, not if, we will experience a pandemic disease of similar virulence as the 1918–1919 flu pandemic, or the Spanish Flu, when, according to the Center for Disease Control (CDC), more than 2.5 percent of the global population died. Though many companies did include such scenarios in their ERM programs, most approached it with a bit of skepticism. This is no longer the case. As the 2009 flu season approached, there were significant fears that the impending H1N1 flu pandemic might be as deadly as the 1918 flu. Although it turned out to only be about as deadly as a typical seasonal flu, this experience changed attitudes. Before H1N1, the fact that an ''old'' date (1918) was attached to the deadly event made it seem more unlikely or unreal to us.

Pirates

Though not a particularly important factor, piracy is worth mentioning because it is another example of something that previously seemed unimaginable in modern times. However, in 2009, pirate attacks off the coast of Somalia received a lot of media attention and became a concern for the shipping industry and cruise lines. Before this occurred, if you raised this as a potential risk, the response would have been, ''Pirates? Are you kidding?'' Pirates evoke a far distant history of wooden ships and cannon. It had been over 100 years since the last attack on a U.S. ship by pirates. Yet, again, a remote (and ridiculous-sounding) risk event becoming reality is more fodder for ERM programs, which include exercises to identify emerging risks—risks currently not on the radar screen but that might become important in the future. Events such as this have made us more aware of the gap between our attitude before a remote event occurs and immediately afterwards, and how quickly our mind-set, and our reality, can change.

LONG-TERM TRENDS

In addition to the events laid out chronologically earlier in the chapter, there are two other drivers of ERM adoption worth mentioning that have evolved over a long period of time. One is technological advancement. ERM requires a lot of computing power. Until recently, the run time for the required calculations was prohibitively slow. However, the continued increase in processing speeds is now making ERM feasible, and companies are beginning to take advantage of this.

Another driver is increased risk savvy in the business world and even in the general population. Until fairly recently, consumers of information have been content to receive ''best-estimate'' projections, be they earnings forecasts or weather forecasts. However, in recent years, consumers have become more comfortable with the concept of volatility (the best estimate does not always occur) and also more accustomed to receiving and processing multiple scenarios (ranges of possible results, either above or below best estimate). As a result, forecasts have taken a more sophisticated turn and commonly provide a range of possible or likely occurrences. For example, television weather forecasts of hurricanes routinely display a range of possible paths, often with color-coded probability ranges produced by sophisticated weather models. Another example is media coverage of elections,

where analysts now present consumers with numerous detailed scenarios that might influence different results.

CHALLENGES TO ERM

As a result of all the factors driving awareness and adoption of ERM programs, ERM is currently a hot topic, and has been for a few years. Most companies have begun adopting ERM, are considering adopting ERM, or are curious to learn more about ERM. Boards of directors are asking about it, and their management is actively seeking knowledge about it. Even non-profit organizations and government entities have an interest in ERM and how they can adapt it for their use. At companies implementing ERM, many have a formal full-time position of chief risk officer (CRO) to lead the development, implementation, maintenance, and enhancement of the ERM program.

In response to this demand, providers of products and services have been rapidly investing in growth to serve the growing ERM market. Conferences are adding ERM as a topic to their agenda or offering entire events dedicated solely to ERM. Universities are building ERM curricula for executives as well as students, and are searching for both content and qualified professors. Consulting firms, audit firms, and technology providers are continually seeking to develop and expand their ERM products and services and are competing to hire ERM practitioners from the limited pool of qualified people.

With all this momentum, it may seem inevitable that ERM will become a large and sustaining movement in the corporate world and beyond. However, there are two major challenges that currently threaten to derail the ERM movement:

1. Confusion over ERM providers
2. ERM programs falling short of expectations

Confusion over ERM Providers

The first challenge is confusion in the market over just what ERM is and who is offering valid ERM services. The rapid proliferation of providers of ERM products and services has resulted in many ERM providers that narrowly define ERM in a way that plays to their limited set of products and services, which are usually risk management offerings that pre-date ERM. This confusion over what constitutes ERM may also lead to the tarnishing and eventual abandonment of the label *ERM*, although the valid underlying ERM concepts would live on

under a new name. Chapter 2 addresses this by providing a robust definition of ERM, which can be used to evaluate whether a company's risk management program is, in fact, an ERM program. Another result of this confusion in the marketplace for ERM products and services is that it may dissuade some companies from adopting ERM.

ERM Programs Falling Short of Expectations

The second challenge is that the majority of ERM programs are falling short of expectations. There is no consensus yet on ERM best practices, and there are a variety of methods being employed. Most ERM frameworks and approaches currently in use, while producing some valuable benefits, are resulting in suboptimal ERM programs. Chapter 3 defines the ERM framework for an advanced yet practical approach that helps companies avoid these issues and successfully implement a robust ERM program. The majority of the book describes this framework and approach in more detail.

SUMMARY

Due to a confluence of significant risk-related events, mostly over the past 10 years, as well as longer-term supporting trends, the time for ERM seems to have arrived. Some disastrous events, both man-made and natural, have raised management's awareness of specific sources of risks, the possibility of worst-case scenarios, and the need for an integrated approach to managing risk. Some actions, both proactive and reactive, by external stakeholders—rating agencies and government bodies—have improved risk management practices and disclosures, as well as raised management's awareness of the benefits of an ERM program. While poised to continue to grow as a business approach, ERM suffers from some confusion in the marketplace and a lack of leading practices. In the next chapter, we will begin to clear up some of this confusion by thoroughly and clearly defining ERM. The remainder of this book will then go on to delineate leading practices for ERM.

NOTES

1. Basel II replaced the original Basel Accord. While there is now a Basel III emerging, it is not materially different, from the perspective of our discussion. The primary difference is higher capital requirements.

2. ''Definitive Statistics Comparing Driving with Flying,'' available at www .fearofflying.com/about/research.shtml#driving. The study indicates that such an increase in terrorism would make flying about as risky as rural interstate driving, which is one of the least risky types of driving. Therefore, overall, driving would still be riskier.
3. ''How We Calculate Risk: Fear of Flying After 9/11 Led to Increase in Auto Deaths,'' available at http://thestatsblog.wordpress.com/2008/01/16/fear-of-flying-after-911-led-to-increase-in-auto-deaths/.
4. The COSO Internal Control framework is intended as a process to help achieve effectiveness and efficiency of operations, reliability of financial reporting, and compliance.