

Part One

WHERE WE ARE NOW

<http://www.pbookshop.com>
COPYRIGHTED MATERIAL

<http://www.pbookshop.com>

Chapter 1

Surviving a Series of Unfortunate Events

As we left the twentieth century and welcomed the beginning of the twenty-first, the world economy appeared to be in greater shape than ever before. Things were probably going well for you, too. You had an enjoyable job, working for a first-rate company. Every day you looked forward to your commute. On any given morning, you would make your way downstairs to your front door to be the first to take the morning's newspaper. Opening the paper, you would read the headlines. Let's take a look at the following news headlines and consider how much you or your company's board members would like to see headlines like these about the first-rate company for which you worked:

Exxon Takes a Spill in Alaska

Newsday *April 2, 1989*

Heads Roll at Showa Shell

The Independent – London *February 26, 1993*

Kidder Scandal Rocks Wall Street

The Plain Dealer *April 19, 1994*

NASDAQ: An Embarrassment of Embarrassments*BusinessWeek* November 7, 1994**A Big Bank Goes Belly Up***Los Angeles Times* February 28, 1995**How Many Other Barings Are There?***Wall Street Journal* February 28, 1995**Boss Resigns as More Daiwa Losses Emerge***South China Morning Post* October 10, 1995**Enron Falls—With a Whimper***Miami Herald* January 16, 2002**Andersen, Enron Get Federal Review***Washington Post* January 26, 2002**Allied Irish Plunges after Suspected Fraud***Reuters News* February 2, 2002**MCI Expected to Pay Massive Fine in SEC Deal***Wall Street Journal* May 19, 2003**Citigroup Private Banks Kicked Out of Japan***New York Times* September 20, 2004**Prudential to Pay Restitution and Fines of \$600 Million***Deseret Morning News* August 29, 2006

Note that these headlines not only point to the financial impact on companies, but also have consequences beyond their earnings—from the personal to the greater community. Many people, especially those never involved in any wrongdoing, have been hurt and even ruined. Aside from resulting in headline news and adversely affecting a variety of industries and thousands of people, these obviously independent and unfortunate events have something else in common. Let us examine one of the more famous cases to help us better understand this unique commonality.

Crime of the Century

On February 26, 1995, Barings Bank, the oldest bank in Great Britain, was unable to meet its funding requirements and was declared bankrupt. Barings was founded in 1762, helped finance the Napoleonic Wars, the Louisiana Purchase, and the Erie Canal, and 233 years later,

on March 3, 1995, the Dutch Bank, ING, bought it for a total of £1.00. How did something like this happen? Virtually all of the stories about this subject blame one man: Nick Leeson. These stories, often told and retold, are virtually the same.

Nick Leeson grew up in a suburb of London, England, and first worked for Morgan Stanley. He later joined Barings and was asked to fix an operations issue in their Indonesia office, which he successfully accomplished within a year. As a result of this, he was moved to the Barings office in Singapore, and then by 1993 was promoted to general manager of that office, giving him authority over both the traders and the operations, or back office, personnel. He then passed an exam that allowed him to trade on the Singapore Mercantile Exchange (SIMEX) and then acted in the capacity of a trader, in addition to managing other traders and back-office personnel.

Leeson was an unlucky, or perhaps a poor, trader and began to mount major losses. He was able to hide these losses in an error account and show profits in his trading accounts. Being the head of both the front and back offices, he was the senior person to review both the trading and error accounts and decide what to report to Barings management at headquarters. Once Barings's senior management realized what had happened, the bank's losses had accumulated to \$1.4 billion, and Barings was not able to meet its cash obligations to SIMEX, resulting in bankruptcy. Meanwhile, Leeson had fled the country and then was found and arrested in Frankfurt, Germany, on March 3, 1995, the same day ING purchased Barings for £1.00 (or \$1.60 at that time).

Leeson was convicted of fraud and sentenced to six and a half years in a Singaporean prison. During this same time, statements like the following were made in many articles and magazine articles:

- "One man single-handedly bankrupted the bank that financed the Napoleonic Wars. . . ."
- "The failure was caused by the actions of a single trader. . . ."
- "The activities of Nick Leeson led to the downfall of Barings. . . ."
- "Leeson, acting as a rogue trader, accumulated over a billion in losses. . . ."

Even Leeson himself admitted his guilt, and while in prison he wrote a book on the subject, entitled *Rogue Trader: How I Brought Down*

Barings Bank and Shook the Financial World. That book was then made into a movie, called *Rogue Trader*, starring Ewan McGregor as Nick Leeson. And finally, *TIME* magazine includes the collapse of Barings among the top 25 crimes of the twentieth century!¹

Yet these stories and newspapers and magazines got it wrong. Yes, Leeson had engaged in unauthorized trading for over two years and exposed the capital of Barings Bank to almost unlimited potential loss. Yes, he committed fraud and needed to be punished for that crime. And yes, he took full responsibility for his actions, pleaded guilty, and spent time in jail. However, the collapse of Barings Bank cannot be placed squarely 100% on him. This was not a crime of just one person.

Another View of the Barings Collapse

While the vast majority blamed Nick Leeson as the “lone gunman” that killed Barings, a few dissenters emerged with a different, if not more enlightened, view. One such view, surprisingly, came from England’s Board of Banking Supervision. The Board operated under England’s 1987 Banking Act and then was subsumed within the Financial Services Authority (FSA) in 1998 (under the 1998 Bank of England Act). Immediately after the Barings collapse, the Board of Banking Supervision was requested by the Chancellor of the Exchequer to conduct an “Inquiry into the Circumstances of the Collapse of Barings” and issued its report on July 18, 1995.² This report paints a different picture of Barings Bank and its senior management. Rather than showing Barings management as a victim of a clever criminal of the century, the Board of Banking Supervision laid the responsibility for the collapse of Barings on the company’s Board of Directors and management.

Beyond what the Board of Banking Supervision concluded, reviewing the facts would lead someone who understands risk management and control to conclude that *Barings management allowed themselves to become bankrupt*. How could this happen? Management of any thriving company would typically want their company to stay healthy and afloat. Barings management did not purposefully drive their company to bankruptcy, nor did they attempt to design a structure that would endanger company profits. This was a case of management inattentiveness and indifference, the results of which were the same as if

management purposefully drove their company to ruin. What did management do or not do? Investigations found several things, including the following:

- Allowing a lack of segregation between front-office and back-office operations
- No senior management involvement
- Lack of supervision
- Poor control procedures

Barings management allowed the lack of segregation between front- and back-office operations, a clear violation of a basic control in every business, especially banking. When Leeson was made general manager, Barings management allowed him to trade while simultaneously supervising back-office personnel—the same personnel who were supposed to *independently* review and process the trades executed by Leeson. What an absurdity—to be the manager of those who are supposed to independently review your work!

Even Barings's internal audit department became involved, as they should in every corporation as a normal course of business. In 1994, James Baker, the internal auditor assigned to review Leeson's operations, noted the lack of segregation of duties (by having the same manager supervise both front- and back-office operations) and recommended in his report that the "back office should be reorganized so that the General Manager is no longer directly responsible for the back office."³ Leeson agreed to this recommendation in writing and then proceeded to ignore it. No one followed up to ensure that the promised action actually took place. This is just one of many examples where senior management did not bother to involve themselves in a significant operation.

On paper, Leeson had several supervisors. In reality, he had none, mostly because no one felt fully responsible for his actions. In fact, when Leeson first began his Singapore business at Barings in 1992, James Bax, the head of Barings Securities in Singapore, complained to senior management in London that Leeson's unclear reporting lines would create a "danger of setting up a structure which will subsequently prove disastrous."⁴ This warning was ignored and Leeson was able to march ahead without suitable supervision or direction, without

proper checks and balances. Anyone could easily go astray if even some minimal type of feedback is not provided.

Finally, what control procedures did Barings have in place? At some point in 1993, Barings reportedly tried creating a risk committee to review trading positions. That effort dissipated soon thereafter. Then, in April 1994, Barings management read the news of Wall Street trader Joseph Jett of Kidder Peabody, who created false profits of \$350 million, resulting in major losses for that company. In response, and like many other financial services firms, Barings management began to review its controls in an attempt to prevent a similar incident at their bank. Even though control inadequacies were found, no changes were made. This is not surprising. A company that was willing to have a trader in a satellite location unsupervised with management oversight for both front- and back-office operations would not only be lacking in control procedures, but also unwilling to make the painful, yet important, changes necessary to ensure a return to some control over its risk.

Therefore, the eventual collapse of Barings Bank, whether brought into the open by the antics of Nick Leeson or by some other person, was due to the lack of controls at Barings Bank. Moreover, the collapse of Barings was due to the bank's lack of *operational risk management*.

A Story Closer to Home

The Barings story is truly fantastic and one that hopefully would not be repeated at another company, if its lessons were truly and fully learned. In fact, these are life lessons that need to be applied to all parts of business. Consider the following fictional account that could be happening at your company. Granted, this is a small event, and purposefully so. Such things may happen often and you are not aware of it. Perhaps what is happening at your company is not exactly like this incident, but something close. . . .

Ken Clarkson has been very happy in his three years at Unicon Inc. He moved from operations to sales just a few weeks ago and believes that he is moving up in the company.

"Here you go, Ken." Alicia, the sales department's administrative manager handed him a familiar white envelope. "Your first official paycheck in sales."

He laughed as he took the envelope from her. While it was his first time being paid in his new department, it was the same process throughout Unicon. The envelope did not contain a check, but instead a statement of his earnings for the past two weeks, noting gross earnings, deductions for federal and state taxes, insurance and 401(k) benefits, and finally net earnings. Being a progressive company, Unicon places all of its employees on electronic direct deposit, thereby preventing losses and mistakes with printed paychecks.

“Oh, look at this,” said Alicia. “You have a second one.” She handed Ken a second envelope. “Must be some hours left over from your previous department. Or maybe it’s just your lucky day!” She laughed and walked over to another worker.

Ken knew that he was appropriately paid just two weeks earlier, so the second envelope could not be for any hours left over. He opened the first one—everything was what he expected: correct salary, correct deductions, and the correct net amount deposited into the correct bank account. He opened the second—same salary, deductions, and net amount also directly deposited into his bank account.

What should he do?

“Keep it,” volunteered a coworker. “It’s their problem.”

“No,” said a second coworker, “they are bound to catch it sometime and then you’ll be in trouble.”

“You won’t be in any trouble,” answered the first worker. “They made the mistake, and you thought one check was for your time in your previous department.”

This is not a lesson in morals. People act according to their beliefs. In real life, Ken presented the two statements to the company’s payroll department, where he was told “Thank you. We would never have caught this if you did not show us.”

You say: This does not happen in my company.

Think again.

Does your payroll department have controls to prevent double paying an employee? Do payroll employees validate what was actually paid out to what was supposed to be paid out?

You say: Our payroll is all online with no paper, so something like this can’t happen.

Think again.

Do you ever have people being hired, leaving, or changing departments? If so, then each of those events requires a manual effort by someone, and that means mistakes can happen. Additionally, is the access to your payroll system controlled so that only authorized people can make changes? If not, then further problems could occur.

You say: My payroll is outsourced, so my vendor pays for these mistakes.

Think again.

Have you read the agreement with your payroll vendor? Do you know the terms and the responsibilities of each party? Your payroll vendor is responsible only for paying out exactly what you tell the vendor to pay. You are responsible for controls to ensure what you give the vendor is correct. To make matters worse, while your payroll department may not have such controls, it probably checks the vendor's output to what it sent the vendor, which is simply performing the control the vendor is responsible for performing itself.

You say: This is not much money and will not hurt my company.

Think again.

Of course, this is a simplified example. While research on losses due to operational risks is in its infancy, when the Basel Committee on Banking Supervision's Risk Management Group surveyed 89 banks in 2002, these banks reported 47,000 individual loss events with amounts in excess of €10,000 for 2001, or €7.8 billion in total, or an average of approximately €90 million per bank. Clearly, this was just the tip of the proverbial iceberg. When these losses are categorized by event type, frequency, and amount of loss, the distribution would be as follows⁵:

	Percent of Loss Events	Percent of Loss Amounts
Losses due to internal and external fraud	46%	23%
Losses due to other causes, including processes, systems, products, damage, safety, etc.	54%	77%

While fraudulent activities may have exploited weaknesses in processes, systems, and so forth, nevertheless, they represented less than half

of the number of losses and less than a quarter of the money spent on losses. Therefore, mistakes, inappropriate controls and procedures, lack of segregation of duties, and other operational risks cost companies and their shareholders—both in tangible terms as previously summarized and in intangible terms such as lost productivity and lost opportunity.

Beyond the economic and reputation costs, there are even simple survival issues at stake. Witness what transpired at Arthur Andersen, in the aftermath of Enron, where a global accounting firm could be forced to cease operations by the irreparable damage to its reputation caused by one incident. The thousands of employees of Arthur Andersen and Enron became unwilling victims of a series of unfortunate events, showing the cost of highly questionable legal and ethical risks, provoking failures in processes and systems.

The Firefighter and the Fire Marshal

Do you think it would be worth your while to put in simple controls to prevent such mishaps? Incidents like the ones experienced at Barings, Enron, Arthur Andersen, Daiwa, Kidder Peabody, and many others are examples of *operational risk* (i.e., the risk of loss resulting from inadequate processes, people, or systems). This is the type of risk people normally wish to avoid rather than incur by design.

There are times that you or your company will want to take risk. That is normal. Business risk—just taking the risk of trying to make money selling your product or service—is the first thing that comes to mind. There is also market risk, where you buy or sell stock or property and your profit is subject to the ups and downs of the market. Credit risk is another risk you might incur on purpose. You or your company may loan money to another person or company at some interest rate. You now have taken on the risk of that person's or company's being able to repay the loan plus interest.

However, operational risk is a type of risk that you do not want to take on. It is everywhere around us and in every action of a company—when a company agrees to mail you a book you purchased over the Internet, when a company operates a factory in a community that may complain about noise or pollution, and on and on.

Your company may be good at fixing problems when they arise. How good is it at preventing problems in the future? Prevention—that

is, managing and controlling operational risk—is important to reducing a company’s costs and protecting shareholder value. Even more important is to learn how to manage this risk now, to prevent future loss incidents.

A dramatic but familiar analogy of the difference between fixing and preventing problems is what differentiates a firefighter from a fire marshal. The firefighter works very hard to put out fires, to stop fires from spreading, and to reduce the number of people and property hurt by the fire. The fire marshal is responsible for the investigation and prevention of future fires. This analogy can be applied to companies—all companies have firefighters. Do they have fire marshals?

We do not intend to improve your company’s firefighting abilities. We are sure that your company has excellent firefighters, helping to fix a problem or remediate a broken process. You may be a firefighter yourself.

We do not intend to argue for fewer firefighters. Fires will always happen, and firefighters will always be needed.

Our intent is to help your company develop fire marshals. This book will provide you with the tools needed to be an operational risk manager and to investigate your business processes in order to prevent future operational risk losses. In doing this, we will examine the following questions that are essential to a company’s well-being in the twenty-first century:

- Do you understand operational risk, how it affects the bottom line, shareholder value, reputation, and even survival, and what you face today if you wish to manage this risk?
- Does your company have an inventory of its key business processes with documented controls and designated senior managers responsible, and how is operational risk taken into consideration when processes are designed?
- Does your company have a technology inventory with procedures and controls over application integrity, access, and data, and how is operational risk taken into consideration when technology solutions are designed or acquired?
- Does your company have an inventory of its key outsourcing relationships with documented controls and designated senior managers responsible, and how is operational risk taken into consideration when entering into these relationships?

- Does your company have an operational risk management or control function?
- How do you or would you organize an operational risk management group in your company?
- What relationship does or should your operational risk management group have with corporate management and other control areas, such as compliance, finance, and internal audit?
- What corporate governance does your company use for approving, implementing, and monitoring products, services, and processes?
- To what extent does your company link employee compensation or job performance to operational risk management?

Answer these questions, implement an operational risk management structure within your company, and imagine seeing the following headlines about your company over the next decade:

{Your Firm} Escapes This Year's Accounting Scandals

Wall Street Journal *Someday, 2010*

Annual Review: {Your Firm} Stands Alone in Service Excellence

BusinessWeek *Some week, 2012*

Fifth Year of Record Profits for {Your Firm}

New York Times *Someday, 2015*

Why Does {Your Firm} Keep Winning Awards Every Year?

The Economist *Some week, 2020*

How Do We Get There?

What can one do about the risk of loss resulting from inadequate processes, people, or systems? Let us begin with people. People accomplish their work and deliver business results, good or bad, through their activities. Activities, in turn, are the building blocks of processes. If employees correctly and completely perform their critical activities and business processes in support of the business, there should be reduced opportunity for loss. So, one can say that losses incurred by people, except for blatant, willful, and malicious losses, are really losses that might have been avoided and more quickly detected if their

activities were organized or monitored through more effective design and management of business processes.

Similarly, systems are generally implemented to support, enable, or otherwise facilitate business processes. Losses incurred due to systems might also be avoided through more effective design and management of the business processes calling for such systems and the system life-cycle management processes with which the systems are developed.

Finally, noncatastrophic external events, such as customer returns, especially when they appear to be trends, are probably the result of a business process that either failed to correctly determine customer needs or expectations, or failed to deliver a product or service that fulfilled those correctly known needs and expectations.

Therefore, given the foregoing, it does not seem far-fetched to suggest that designing and managing business processes is a critical factor to develop and implement successful operational risk management. In fact, since operational risk management is itself a business process, the principles of effective business process management should be applied to the design and implementation of the operational risk management process.

Over the next several chapters, tools for operational risk management and business process management will be introduced and explained. We will provide commonly used tools, plus new tools designed by the authors. Finally, by combining these new tools, a new integrated concept and framework will emerge to help risk managers—the corporate fire marshals of the twenty-first century—to be prepared. Exhibit 1.1 provides a sneak peek at this integrated framework.

We aim to help corporate fire marshals—new ones and even existing ones—who seek additional answers. This will be accomplished by first explaining operational risk management and business process management. Then, we will examine how one can integrate the two management processes into one framework. Finally, each of the several elements of this integrated framework will be explored, showing how to apply these concepts and working models into real practice. As a result, this book will help you understand operational risk, demonstrate to you the criticality of business process management to operational risk management, and deliver to you the tools you will need to successfully manage and mitigate operational risk in your business, your home, and your everyday life.

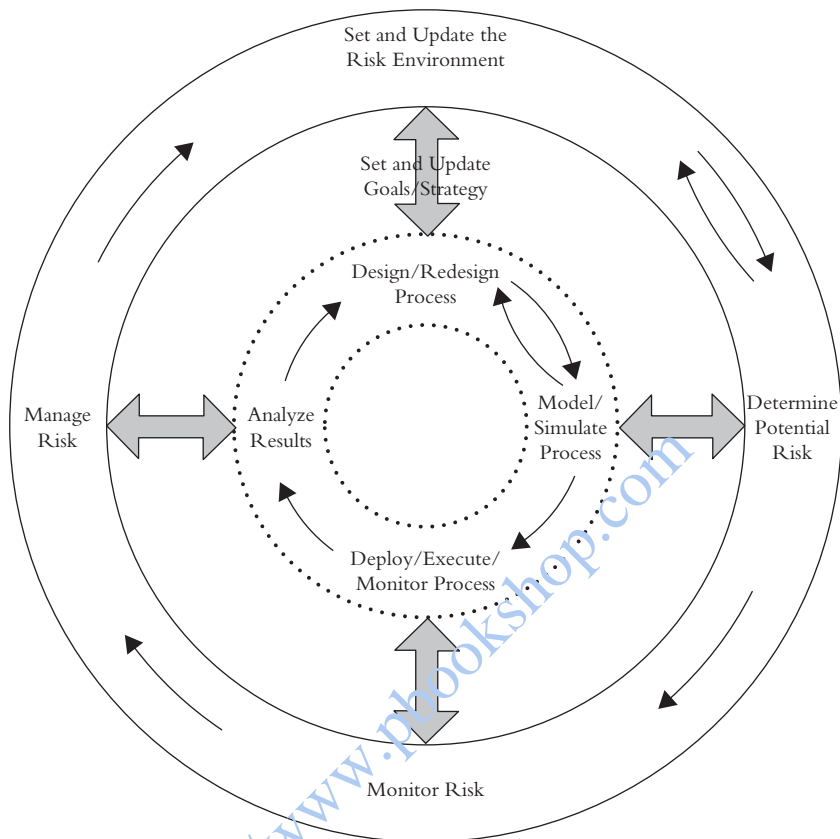


Exhibit 1.1 Integrating Operational Risk and Business Process Management

Notes

1. Howard Chua-Eoan, "Top 25 Crimes of the Century," www.time.com, Time Inc.
2. Board of Banking Supervision, "Report of the Board of Banking Supervision Inquiry into the Circumstances of the Collapse of Barings," London, England, 1995.
3. Ibid.
4. Barings Securities (Singapore) fax dated March 25, 1992, from James Bax to Andrew Fraser, Board of Banking Supervision, "Report of the Board of Banking Supervision Inquiry into the Circumstances of the Collapse of Barings," London, England, 1995.
5. "The 2002 Loss Data Collection Exercise for Operational Risk: Summary of the Data Collected," Basel Committee on Banking Supervision, Basel, Switzerland, March 2003.

<http://www.pbookshop.com>