2008

Smart risk management : a guide to identifying and reducing everyday business risk

Ronald Rael

SMART RISK MANAGEMENT

Ron Rael, CPA

AICPA

SMART RISK MANAGEMENT

A Guide to Identifying and Reducing Everyday Business Risks

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

AICPA®

Ron Rael, CPA

SMART RISK MANAGEMENT

A Guide to **Identifying** and **Reducing** Everyday Business Risks

American Institute of Certified Public Accountants

Ron Rael, CPA
Leadership Coach

1911-356

Notice to Readers

Smart Risk Management: A Guide to Identifying and Reducing Everyday Business Risks does not represent an official position of the American Institute of Certified Public Accountants, and it is distributed with the understanding that the author and the publisher are not rendering legal, accounting, or other professional services in this publication. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

1 2 3 4 5 6 7 8 9 0 PP 0 9 8

ISBN 978-0-87051-749-5

Preface

The goal of your risk management program is to ensure the continuity of the business and answer this crucial question:

What could disrupt your business model or harm your firm's earnings potential?

Controllers and CFOs must be able to define the payoffs from business-risk-taking and to explore the methods of understanding, identifying, and reducing the negative effects of everyday business risks. By reading this book, you will define business-risk-taking and learn to follow a formal process to handle risks better.

This book is designed for any decision maker who recognizes that too much effort in controlling risks hurts innovation and not enough control is wasteful and expensive

After reading this book, you should be able to

- analyze risks.
- discuss how to plan for risks.
- understand how to reduce the potential negative impact of risks.
- understand the 50 risk tools and how to use them.
- apply the 50 tools to meet the requirements of Sarbanes-Oxley.
- help others take risks and be more innovative with less costly downsides.
- see risk taking in an entirely new way.

Contents

Exercises

Introduction

The Ultimate Risk Taker

> *Who would you say is the ultimate risk taker? Who is someone you know who takes the sorts of risks you admire?*

Keep this person in mind as you read the following story of the person I believe is the ultimate risk taker: Walt Disney.

If you are not familiar with the story of how Disneyland was created, I will recap its history and tell you about Walt Disney. In the 1940s and 1950s, Walt was a film producer in Southern California and usually worked six days per week. On Sundays, he liked to take his two daughters to amusement parks around the area. Although his daughters enjoyed the experience, Walt did not. He and the other parents would sit around with nothing to do while their children were having fun. Most of these amusement parks were dirty, poorly maintained, and sometimes even unsafe.

During this time period, Walt took his family on a tour of the Bavarian Alps and what he saw there really affected him. He fell in love with the castles, the clean cities, and the friendliness of the people. He felt inspired by the Tivoli Gardens in Copenhagen.

These two situations hung around in Walt's creative mind. Soon afterward, he came up with the concept for Disneyland. Like many ultimate risk takers, not everyone immediately buys into their vision, and the same was true for Walt Disney.

When Walt sought financing for his dream of Disneyland, bankers turned him down. He approached other investors who did the same. They asked him questions like: "Why would anybody want to pay lots of money to go to an upscale amusement park? Why would anybody want to travel miles into the orange fields of an out-of-the-way place called Anaheim?" (Anaheim today is nothing like it was in 1950 and probably would not be if it were not for Walt Disney.)

The visionary Walt was tenacious, like all ultimate risk takers, so he persisted toward fulfilling his dream. He was approached by ABC studios to create a children's television program. Walt agreed to develop one only if they would be willing to finance his concept of an amusement park.

What most people do not know is that Walt ran out of money before Disneyland was fully completed. Several sections were incomplete, Matterhorn Mountain among them. Walt wanted exotic trees all around the park, but ran out of funds before he could purchase them. So he used local trees marked with exotic names—no one noticed!

Disneyland opened as Walt had promised in 1955. Opening day was a fiasco because all kinds of things went wrong: rides broke down, they underestimated the amount of visitors, and they ran out of food.

If you look at Disneyland today, however, you can see that it exceeds even Walt's original vision. Disneyland was not "because of a mouse," as Walt was fond of saying; instead, it was due to his dream, his willingness to take a huge risk, and his tenacity.

We will examine risk in a different way than you are accustomed. Most of us CPAs and financial-types think of risk management in one of two ways: either as the concept of risk taking on an individual level or as buying insurance and making sure to have sufficient coverage if a disaster occurs. What you will discover today is that risk management is much more. We tend to focus on the small view. The goal is to take you on a journey so that you will understand what true risk management is all about.

This book provides you with 50 different tools to use and 6 specific steps to follow so that your organization or client does a better job of managing business risk. The biggest "Aha!" in understanding risk management comes when you embrace the fact that while one side of risk management involves protecting the company from the downside of risk, the other side involves being willing to take that risk.

"Oh no! Don't tell me we have to cover that—I hate taking risks!" is what you might be thinking by now.

Sorry! You are not really able to be innovative unless you do risk planning. In order to do a good job of leading an organization, you must look at risk taking and understand what risk taking means on three levels: the individual, the corporate, and the global. You will end up with an understanding of risk from a senior leader's point of view.

Exercise: What Is Your Risk IQ?

Instructions

Complete this self-test to see if you are adequately managing the everyday risks that your firm faces. Place a checkmark next to the questions that you answer with a definite "Yes." Compare the total number of boxes you checked with the answer key at the end.

___ Am I able to sleep at night without worrying about risk in my organization?

___ Do I have a clear understanding of firm-wide risk, the organization's key areas of vulnerability, and our ability to recover quickly?

___ Am I confident that an accountable executive is addressing each risk, large and small?

___ Is there a process or function within my organization that is responsible for assessing, measuring, and monitoring risk?

___ Have we created a realistic balance between innovation and protection?

___ Do our cultural norms help us ensure that all costly risk is identified before we take it?

___ Does my organization have an operational system or process for evaluating risk?

___ Do I have complete assurance that financial and operational controls are being used as designed?

___ Does your organization have a thorough and appropriate system with timely reports that use checks or balances on innovation, fraud prevention, and risks faced?

___ Do I have assurance that financial and other information is reported correctly?

___ Are our processes for risk assessment, management control, and governance being evaluated and reviewed for both efficiency and effectiveness on an ongoing basis?

___ Is there an emphasis and supporting process within my organization for aiding productivity and for improving operations?

___ Are my organization's stakeholders provided with reliable assurances that their investment is protected by ethical and sustainable means?

___ If I were not part of the organization [firm's management or the board], would I be comfortable with the assurances provided to me (as a stakeholder or investor)?

___ Do we have a specific written recovery plan in the event that we suffer from a major risk failure?

Answer Key

13–15 checked—Congratulations!

You have a high Risk IQ! Keep doing what you are doing and improve those areas you did not check off.

10–12 checked—Good job!

You are effectively managing your risk, but are still vulnerable in many areas. Get started on removing those weaknesses today.

7–9 checked—Scammers love you!

You have so many areas of vulnerability that fixing these vulnerabilities will be like trying to empty a full bathtub with a teaspoon. Get cracking!

0–6 checked—Sharpen your resume!

Your company will be out of business within two years. Ouch.

1

What Risk Management Is and Is Not

Risk management is not *simply having adequate insurance!*

After reading this chapter, you should

- understand what risk management is truly about.
- understand the 5½ steps of proper risk management.
- be able to get yourself into the correct frame of mind about risk management.
- recognize the importance of being innovative in today's business world and global economy.

Getting Into the Risk Mentality

Exercise: Your Risk

To get you into the correct frame of mind, please write down a specific risk. Think of a risk that your organization is undertaking or considering:

- What is the risk, both the upside and downside of it?
- Where is the greatest potential for costly risk?
- What makes this venture or activity risky?
- Why are you concerned about it (as the CFO, controller, or auditor)?
- What concerns do others in your organization have around this particular risk?
- What are the implications or impact on your business or organization if the risk fails?

Keep referring to this risk as you go through this book. You will be able to understand how the tools work by applying them to your specific risk.

No Insurance Selling Allowed!

Whenever this topic is presented to CPAs, accountants, or business managers, the first thing they think is: "This person is trying to sell insurance." Having adequate insurance coverage is only one infinitesimal piece of risk management, which you will soon discover. In fact in this entire book, there is only one small section devoted to insurance coverage.

Christopher Grose, a consultant with the firm Risk Controls Group, best articulates what risk management is all about. Mr. Grose was quoted in a business magazine stating, "Risk management is all about helping you to take the risks ... not to avoid them but take them in the knowledge that you can handle them."

Risk Is Something CFOs Often Ignore!

A survey of 400 leading companies asked: "How prepared are you to protect your revenue drivers in case of a major business disruption?" The survey took the pulse of both risk managers and CFOs.

In the answers, the list of the greatest sources of risk was diverse, especially telling was how much the risk managers and CFOs differed on the sources. It showed a gap between how they each defined the management of risk.

The professional risk managers concentrated mostly on property-related risks, whereas the CFOs included improper management, employee practices, and product recalls in their list of greatest threats:

- 100 percent of the respondents said that a major disruption would have a negative impact on their earnings.
- 28 percent believe that such a risk would threaten their firms' ability to continue.
- 88 percent of the CFOs and 83 percent of the risk managers responded that their company's level or preparation to recover is *less than excellent*.
- 80 percent of all respondents believe that they have not improved their risk management since the events of September 11th.

Anything Can Go Wrong

That is really what real world risk management is about: *having a comfort level that whatever risks come your way, you have the ability to deal with them*. This confidence comes from these three factors:

1. Murphy's first law of "Anything that can go wrong, will go wrong" is a reality. Risk management requires having in place a system or methodology to examine risks before you take them-and I stress the word before. All too often, accounting and finance departments are consulted about a major risk after the risk has been taken. We are called upon to clean up the mess!
2. Employees have tools to examine and measure the impact of a risk. They know how to use them and apply them in their everyday decision making efforts.
3. Leaders all across the firm use insightful information to confidently (as opposed to rashly) step into the unknown.

Every risk has a cost! Are you able to pay that cost?
This is the theme of this book, and it will be referred to often.

Process for Implementing an Effective Risk Management Program

Step 1: Defining what risk is (chapter 5)
Step 2: Examining your attitude toward risk (chapter 6)
Step 3: Analyzing the ability of the firm to handle risk (chapter 7)
Step 4: Minimizing the risk's exposure or downside (chapter 8)
Step 5: Recovering quickly from the negative impacts of the risk (chapter 9)
Step 5$^{1}/_{2}$: Learning something so you can accept even more risk with confidence (chapter 10)

Afford the Cost?

Another example of an ultimate risk taker is Paul Allen, cofounder of Microsoft. Allen is among the richest people in the world. He was featured in a *BusinessWeek* article (May 3, 2004) entitled, "The $12 billion Education of Paul Allen." Allen has lost $12 billion of his net worth in the last decade, while developing as a manager and an entrepreneur. $12 billion!

How many companies can afford to lose $1 million much less $12 billion?

That is the rationale for this book's theme—asking yourself: "Are you able to pay the cost for that particular risk?"

Now I know that some of you are already thinking,

"But, Mr. Expert, you are focusing only on the downside of risk! In almost every risk there is an upside. Are you ignoring that?"

This book was written particularly for CPAs because, as accountants, we often see the downside of risk. Before the upside of risk taking is addressed, let me ask this question. Think seriously as you answer it:

Let us pretend that you just won the lottery today: *"If you won $12 million and were now a multimillionaire, how different would your life be?"*

The following are some typical responses:

- "I will suddenly discover relatives I didn't know I had."
- "Every charity in the world will have my unlisted telephone number on their speed dial."
- "All kinds of people will be asking me for money, even people I do not know!"
- "I will have to make serious choices about what I am going to do from now on."
- "I will have to decide if I should work or not!"

Most importantly, you will have to decide how your life is going to be different from this day forward.

Do you see the cost for you in winning $12 million?

Most of us would answer: *"Yes, having access to $12 million (about $5 million after taxes) is worth the cost!"*

This is the price you must consider whenever you buy a lottery ticket. Your costs include losing your anonymity, being in the limelight whether you like it or not, knowing that you will need to be more proactive with your investments, and having to gratefully pay another CPA to give you financial advice.

Even in the upside of risk taking, there are costs that must be assessed and weighed. This is what risk management is about and why we will most often address the costs and downsides. The tools I give you will address both sides of the cost/benefit ratio for taking risks.

Analysis of Google's Risk

In the same *BusinessWeek* issue, there was an article that focused on Google and what would happen to it once it decided to go public, in particular, the significant risks the firm faces. A major risk relates to its unique culture. Google currently has an extremely employee-friendly culture where employees enjoy lots of perks and high pay. Google hires for talent and not for positions. If they find valuable talents, they hire those people and create positions for them. The article questions whether that culture can continue in light of competitive pressures and analysts' demands for constant cost-cutting.

Another risk is Google's culture of openness. As a public company, the firm will subject themselves to the rules public companies face about disclosures and their impact on share prices.

Another major risk is one faced by the two X-gens who started Google, Sergey Brandt and Larry Page. They both have a free-wheeling attitude as risk takers and (according to the article's author) they are going to soon find out that they will have a lot more accountability for their actions.

None of Google's risks are good or bad—they just need to be addressed. A question I would put before Sergey and Larry is: "In exchange for the millions you generated from going public, are you willing to pay the price of less openness, more accountability to others, and changes to your great company culture?" They would and have answered "yes" (the initial public offering was completed in 2005).

Google's culture will be very different, with less risk taking as time passes. That is part of the cost of being a public and very visible company whose shares are highly prized. The value of each share in late 2005 approached $600! The entire leadership team of Google appears, according to journalists who follow Google closely, to have adjusted to the public scrutiny.

One major change in their culture is one I predicted long ago as a risk–entitlement. For years, employees were given perks such as free lunches, and so on. Now that the cost of these "freebies" is being scrutinized, Google employees feel they are a right and not a privilege. This is causing employee dissension and unhappiness.

Even the simplest things can turn into a risk!

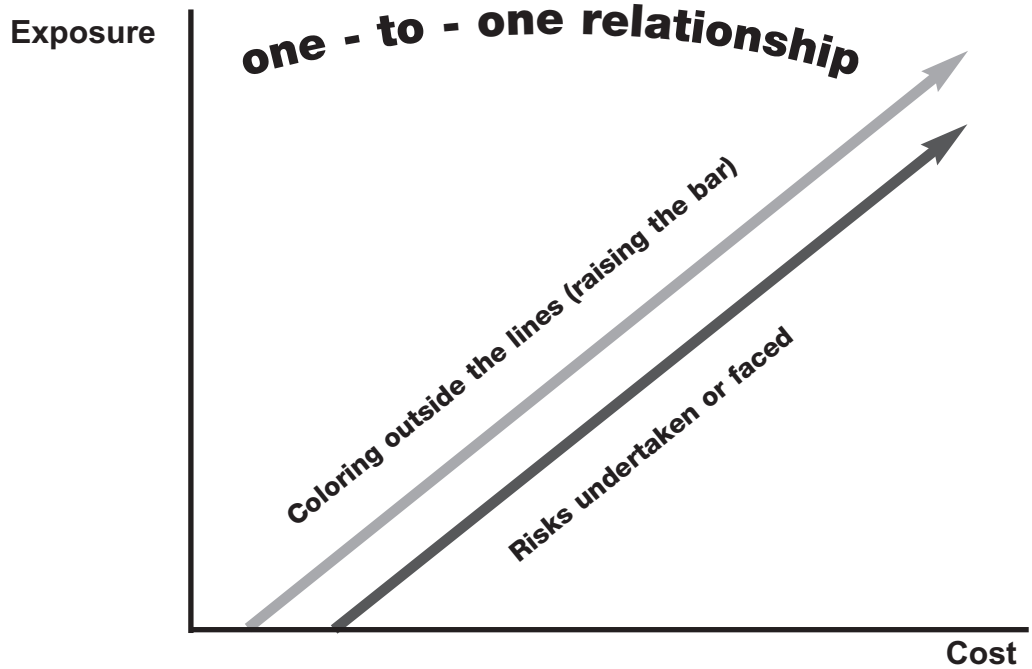
This is part of the cost of being a public and very visible company whose shares are highly prized. But even that creates risk. In late 2005, Google's share price was nearly $600. In July 2008, the price was hovering around $475.

This is what risk taking and management is about.

Relationship of Risk and Risk Taking

As shown in exhibit 1-1, there is a direct, or one-to-one, correlation between risking and the amount of the risks undertaken. The more a firm raises the bar or "colors outside of the lines" on its reputation and requires employees have a willingness to stretch themselves, the greater are the exposures and downsides to the risks taken. Unfortunately, many entrepreneurs and owners of small to medium-sized businesses do not find out about this one-to-one relationship until it is too late. The people who suffer from this expensive wisdom are the firm's employees, investors, and creditors.

Exhibit 1-1
Relationship Between Innovation and Risks Faced



Innovation and Risk Management

Innovation is and has always been an important driver in America's economy.

Risk taking is fundamental to your firm's ability to create value.

Organization leaders have an important role in supporting innovation within their organizations. Innovation is defined as a novel way of doing something that is useful. Creativity refers to thinking in novel or new ways, but in today's new global economy creativity is not enough! Innovation—making creativity useable—is required in order to be competitive and maintain long-term strategic advantage.

Today, there are actually three kinds of innovations fueling our economic growth:

1. Innovations in technology
2. Innovations in business models
3. Innovations in management practices

All three innovation types overlap to an extent, because management practices are the foundation for supporting the first two. In other words, if you have a strong, forward-looking, and strategically aligned management team, your firm will be more likely to have a culture of innovation that is built around a strong and viable business model. Because management practices are critical to innovation, this is where your leaders need to spend their time.

Update the Culture

For many of today's organizations to be innovative, it requires nothing less than an entire revamp of all management practices. The old values of scale, efficiency, automation, and replication are being replaced by an era of imagination, experimentation, and flexibility. These newer values create today's market leaders. The old thinking of caution and careful analysis has been replaced by energy, ideas, and rapid execution. If you doubt this, take a look at those companies that have significantly increased in market value within the last decade: Dell Computers, Stirling Energy Systems, Whole Foods, Univision, Cisco Systems, Getty Images, Amazon.com, Sterling Savings Bank, Starbucks Coffee, Google, Yahoo, Herman Miller, Airbus, Virgin, SBC [now AT&T], and, most recently, Chipotle's Restaurants.

Understanding the Innovative and Risk Taking Organization

These are traits by which you can identify an innovative organization. (Apply this test to your firm.) Do you have

- a compelling vision? _____
- entrepreneurial attitude? _____
- equity compensation? _____
- meritocracy (you earn your place)? _____
- decentralized decision making? _____
- people over policy? _____
- strategic alliances? _____

By putting all these management practices together, you will see that an innovative culture has these cornerstones:

- People are priority number *one* and are inspired by the big vision to come up with great ideas.
- People are given the support and resources to develop their ideas.
- People are financially rewarded for successful innovation or application of their creativity.
- People are given personal career advancement because of the quality of their ideas.

Survival Creates Infinite Sources of Risk

The world is moving way too fast to have only one set of plans. This is why innovation is not only important but necessary for survival. Today, businesses face a diversity of risks from a variety of sources that are rapidly increasing in magnitude and are driven by the type of business they chose to be in. Whatever the category—such as market, credit, operational, political, or compliance—a question must be asked for each specific risk: "Is our company exposed to it?" If the answer is yes, the next question must be: "What proactive steps should we take to ease our exposure to that risk?"

There are so many sources of risk today that we could spend a full day just on ways to deal with the major sources of risk detailed in chapter 13.

You saw the six steps for an effective risk management program (earlier in this chapter). Here are risk management programs recommended by two organizations well known for the quality of their advice. Please notice how similar these are to the six steps we will go through in this book.

Ernst & Young's Steps to Managing Risk

Ernst & Young's *Business Risk Solutions—Global Enterprise Risk Management* suggests these four steps to create an effective risk management program:

Step 1: Figure out what shareholders value about your company

Then you can identify the processes that contribute the most value and brief shareholders on which ones create value, so you can measure performance.

Step 2: Identify the risks surrounding your key shareholder value drivers

Step 3: Determine how you are going to handle these risks

Handle risks by avoiding, managing, insuring, or hedging.

Step 4: Communicate to shareholders what you are going to do about the risks

Arthur Andersen's Steps to Managing Risk

The once robust Arthur Andersen offered a blueprint of six strategies for comprehensive business risk management. Unfortunately, they failed to apply them to themselves and a certain energy firm that shall remain nameless.

Step 1: Establish Risk Management Infrastructure

Appoint an owner of the risk management process and establish the relationship between the risk management and risk monitoring function. Effective risk management always begins with establishing risk objectives with respect to strategy and significant exposures. Risks are assessed from the standpoint of identifying, prioritizing, sourcing, and measuring their potential impact on the organization.

Step 2: Assess Business Risk

Create a conceptual framework that identifies the full range of risks in order to begin risk assessments. Develop an overview of the most serious risk first and allocate resources appropriately.

Step 3: Develop Business Risk Management Strategies

For a risk management strategy to be successful and receive proper focus, it must link directly to the key strategies of the organization. The risk management strategies of avoiding, reducing, retaining, exploiting, and transferring must be developed for each of the significant risks.

Step 4: Develop and Implement Risk Management Techniques

Under a comprehensive approach, an organization implements consistent risk management techniques for all principal risks. This requires an appointed owner of the risk management process, as stated in step 1, such as a chief risk officer.

Step 5: Measure and Monitor Risk Management Process Performance

This is often the step in which the organization will rely most heavily on its internal audit function. This step also includes monitoring other functions, such as regulatory compliance and environmental health and safety. However, progressive risk management means seeking to measure risks and linking these measurements to enterprise performance and to increased shareholder value. Ideally, the measuring and monitoring function works closely with the assessment phase in step 2.

Step 6: Improve Business Risk Management Process

Continual improvement and adaptability are essential to lasting success. Sources of improvements to comprehensive risk management include best practices information and candid feedback from risk owners within business units. Improvement also requires sustained measurement of relevant metrics, such as the number and impact of risks handled within the process.

Summary: Risk is Normal and Expected

Risk management is more than just worrying about tomorrow. In today's world, there are so many things that can go wrong to keep you from staying in business and if your company is not innovating, it will not survive. These two realities mean that every organization must have a clearly defined risk management program that gives its employees tools to anticipate the cost or downside of each risk faced.

2

The Two Views of Risk

What you don't know can kill you; what can kill you, you won't know.

After completing this chapter, you should

- see risk and its relationship to organizational decision making from the "34,000 foot strategic level."
- see a risk and its relationship to employee decision making from the "100 yard individual level."
- understand why some employees and colleagues are willing to take risks and why others only see risk in terms of black and white.

Duality of Risk

The corporate culture that fosters smart and innovative behaviors and decisions must have two major components of dealing with risk in its risk management program. One is a global view on the strategic level. The second is a localized analysis of risk on the individual level. If any of your employees cannot adequately define the risk undertaken before they act, the resulting high costs could damage your firm's reputation. Both views are important and support each other.

Every company must now address the potential impact of unexpected events that could have major financial consequences. Not all organizations have a culture that is prepared for the deep analysis, agile detection, and quick response needed for risk management.

In the book *Best Practices in Planning and Management Reporting*, David Axson, vice president of the Hackett Group, offers three reforecasting approaches that leaders can use to address risk:

- Match your desire for detail with your predictive capability.
- Move toward a forecasting process that balances financial and operational drivers.
- Forecast fewer things more often.

The 34,000 Foot View

Pilots who fly the great jets rely on sophisticated instruments to "see" where they are going when they cannot see with their eyes. Similarly, because you cannot be everywhere at once, your corporate culture norms and risk management tools allow you to detect costly or painful hazards.

Risk Scenario Planning Tool

Running through risk scenarios is one sure-fire method to help leaders understand risk and its likelihood at the 34,000 foot level. This helps establish a clear high to low internal metric that represents the acceptable

and unacceptable costs for the organization. The more your leadership team runs through scenarios, the better it will understand the causes and forces of risk. Great information will be found in these scenario discussions. Of course, your leaders need to include not only financial implications of risks (earnings and cash flow), but also operational implications such as brand, reputation, employment, and oversight of regulators and government agencies.

Exercise: Questions to Gauge Your Risk Tolerance

Determine Your Tolerance Level or the Cost You Can Afford to Lose

Before you undertake the next urgent Strategic Initiative or Action Plan, determine the full consequences if you fail to achieve it. Compare the potential losses, including the softer, hard-to-measure ones, against the alleged or expected payoffs.

- *What risk can we afford to take, and what risk can we not afford to take?*
- *When is the risk considered too much for us?*

Measure Your Risk

Adequate risk measurement has two sorts of return on investment and return on innovation (ROI). There are many different ways to measure these ROIs, but make sure, at regular points in time, you know where you are as it relates to the risk you undertake.

- *Why are we undertaking this risk, and why do we believe the payoff exceeds the cost of the risk?*
- *How will we measure this risk to know when to pull the plug?*
- *Who will take responsibility for measuring objectively, and what is that person expected to do with the data?*

Strike a Balance

You cannot be everything to everyone. Stay focused on what you do best, and stick with that as priority number one.

- *What is most important right now?*
- *What have we done best in the past that worked?*
- *What are we trying to become best at in the future?*

The "100 Yard View"

Risk taking is an exercise in using creativity.

Far too many employees have the mindset that they will get punished whenever they stick their neck out or speak out honestly. Change can be implemented more quickly and effectively when people's mindsets are dealt with before system changes. So when we discuss managing business risks, we must also explore risk taking. Each employee has a differing view of what is risky and what is not. You need to establish, for the whole company, what a risky activity is and what makes it risky: what is the cost we cannot afford?

Objective vs. Subjective Risk

Each decision made and every action taken in a business setting involves humans. By extension, every risk is entered into by a person. In business, there are two classes of risks: subjective and objective. Risks in the objective class are those where we can fairly predict a probable outcome in advance. Whenever you toss a coin to decide something, you can predict that 50 percent of the time the coin will land heads up. There is still a risk that the coin will not show the side you want or need, but statistics prove the 50 percent odds. People want all their risks to be objective—predictable!

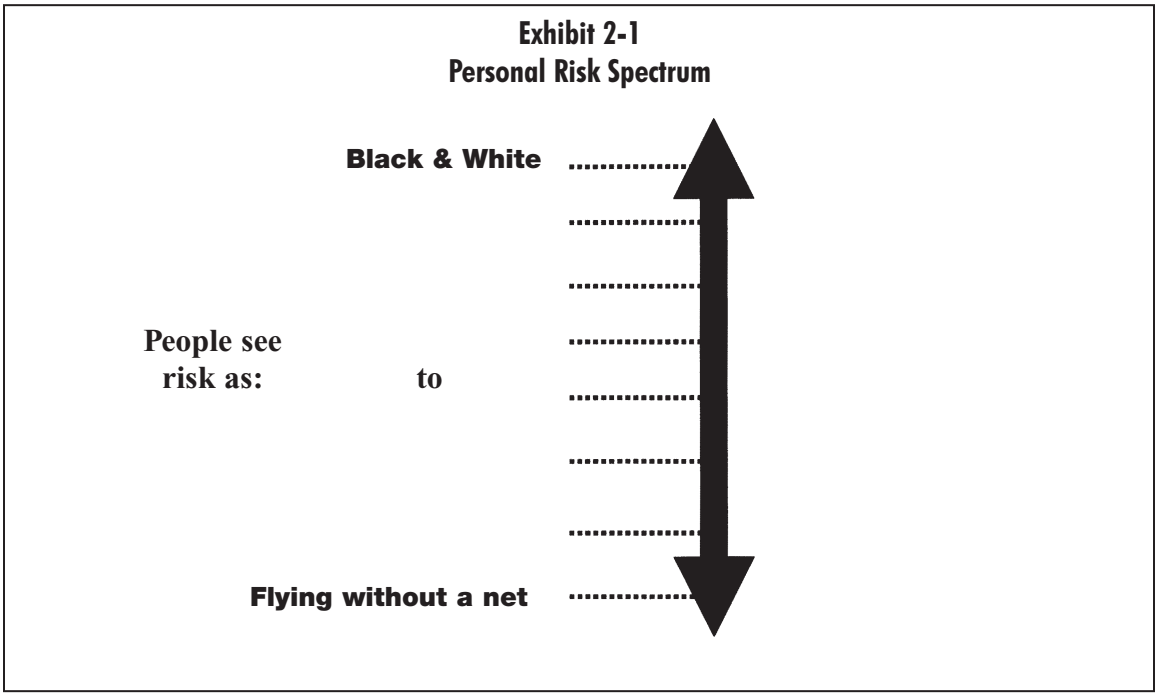
You invest half a million dollars in technology tools but you gain no improvements in productivity or cost savings. This risk you took, despite your best efforts, is the class of risk we face most often—subjective risk. It is hard to predict the outcome and even harder to manage. When you add the reality that we all see risks differently, you can understand why proper risk management must include assessing the human factor when analyzing risks. People do not want all their risks to be subjective, yet Murphy and his laws are alive and well.

What is risk taking on a personal level? Risk taking is a willingness to face our fears and choosing to do or see something differently.

Personal Risk Spectrum Tool

I look at risk taking on the individual level as a range across a spectrum going from "black and white" on one end to "flying without a net" on the other.

Exhibit 2-1
Personal Risk Spectrum



Example: Personal Risk Spectrum

Don is an example of the entrepreneur who has always had an itch to control his own destiny. He retired from a large national organization after 40+ years of placing his career on the black and white side of the Risk Spectrum. Don could not sit still in retirement, so he took some of his pension money and went into self employment. Don found a demand that was not being filled in the industry he knew and loved. His business was quasi-successful until Don recognized an even bigger need that had not been met in the moving industry. His new freight-forwarding business grew very fast, and when he needed help, Don brought his two daughters into the business with him. In just five years, his business went from zero to grossing over $10 million in revenue. Because of his willingness to risk, Don built up a legacy for himself and rewarding careers for his daughters.

True Stories

Some examples to explain this spectrum:

1. If you want to bungee jump, you could say, "I'm either going to live or I'm going to die." That is the black and white view of risk taking. Another time you might look at bungee jumping and see only the thrill and exhilaration of the act. You still know that you might get hurt, but instead your focus is on the thrill and excitement of freefalling rather than what you could lose. Your confidence is based on the knowledge that millions of people who have bungee jumped before you survived. The experience is more important than the cost of what you could lose.
2. In your career, you believe that you have to work or you will be unemployed. So you do not take any risk and do what you must to secure your employment, even though you are not happy in your job. You let being unfulfilled in your job far outweigh the risk or cost of being unemployed. You know there are other jobs out there where you could be happier, but you are not willing to pay the cost of looking for such an employer. Security is so important to you that you see it only one way. This way is looking at the risk of unemployment as a black and white issue.

   In your black and white view of risk, however, you are not able to see that alternatives exist, such as working two jobs or being self-employed. You could search for that second job or start a business while maintaining the comfort and security of a full-time job. By doing so, you accept the cost of taking on the risk that if your main employer finds out, you could end up losing your security blanket.
3. Think of the drive that most entrepreneurs have. Those people rely on themselves to create a business that fills needs that they see are not being met by others. They often give up the security of a full-time paycheck and fly without a net into some enterprise. We often read about the successful CEO who started with a $10,000 credit card and built a viable business in the basement. People who live on this end of the risk spectrum accept the risk or cost of not being cautious at times when they need to be. Another cost they see as negligible is surrounding themselves with like-minded employees or friends who will not or cannot be truthful about the foolhardiness of an idea, decision, or venture.

   Tara had a successful and stable career working for a self-development organization that helps people to grow and become better. After working at this company for many years, she felt that she had done everything she could in her job. Soon after quitting, someone approached Tara with an idea for

a software tool that would help businesses save money. She saw the value of it and borrowed significant dollars to develop the idea into a viable product. Despite investing over a quarter million dollars, the business failed. She never imagined the possibility that she could run out of money before the product was ready to market. It happened. Tara never went back to being an employee, but instead launched a third successful career as a trainer. She continues to "fly without a net."

This Spectrum in My Life

For my history, I can look back and see that many times I saw risk taking as black and white.

I saw going up in a hot air balloon or bungee jumping as dangerous undertakings because I have a fear of falling. Then someone gave me a balloon ride as a gift and I rode in one. I learned that my fear was groundless. I have not bungee jumped yet, but I will. Another example is my fear of piloting an airplane. I believe that piloting an airplane could be difficult for me because I am visually oriented, so I must be able to see where I am going. Yet because I fly a lot, I recognize that the pilots often fly using only instruments.

As it relates to my career and employment though, I have been on "the fly without a net side" of the spectrum. I have always taken risks with my career because I have that entrepreneur drive.

Although security and providing for my family are important to me, the cost of being on my own is less than the cost of a steady full-time job. Even when I was a full-time employee working for others, I ran a side business or worked part-time. At the time I thought I took these risks because of the extra income, but now I realize I needed my freedom and the control of my own destiny.

Fewer Risk Takers

A majority of people tend toward the black and white end of this spectrum. We see fewer risk takers today. I realize that this is a generalization, because people have all kinds of compensating strengths and differing views. It all boils down to individual values and what we hold dear. We use these intangibles in our cost benefit ratio of looking at risk. Often, monetary reward is not what drives people to take risks.

Speaking of money's impact on risk taking, if we look at a gambler who risks $10,000 or even $100,000 on the roll of the dice or the outcome of the game, we can see that gambling fits in the Risk Spectrum. Similarly, look at people who have inherited tremendous wealth and spent it all within a generation. The same varying perspective is true for a person who worked really hard to develop her body into that of a competitive athlete and then later let all that hard work and preparation go to waste. Some of us would see that as a waste or loss. Others would say, "She moved on."

In terms of our friends, we slide across the spectrum. Maybe you socialize only with people who have the same beliefs that you do. Or maybe you have friends from all walks of life who, if you put them all in the same room, would find very little in common. With some friends you would discuss only superficial things; however, with others you would tell your innermost secrets.

In addition to sliding across the spectrum, depending on what we hold as risky, people change this view over time. You know of entrepreneurs who in the early days took all kinds of risks to get their businesses started. Then as they grew more successful and mature in the decision making, these risk takers began to be more cautious and conservative.

Example: Personal Risk Spectrum

Gary is an example of the entrepreneur who started out his career in the black and white spectrum and over time grew frustrated with his lack of job fulfillment. While working for another company, Gary and another employee saw that their firm was underutilizing a product line. The two of them made an offer and, borrowing heavily, purchased that piece of the business. Very quickly they expanded into more markets and have built a very promising and successful business. Yet outside of the business setting, Gary and his partner would be seen as cautious and conservative in most aspects of their lives.

Summary: Everyone Sees Risk Differently

As you can see, there are many different flavors in this spectrum of individual risk taking. As a leader who is trying to build a culture that balances innovation with control and develop employees who think for themselves, you must look at risk through the eyes of your employees. This spectrum tool will enable you to do that.

3

Enterprise Risk Management

Every chain (and enterprise) is as strong as its weakest link.

And every chain has a weak link.

After completing this chapter, you should

- understand the basics of enterprise risk management (ERM) and its evolution.
- understand the continuous cycle nature of ERM.
- be able to explain the payoff of ERM to others in your organization.

Risk Is Something CEOs Often Ignore!

1,400 CFOs of U.S. companies with 20 or more employees responded to a survey on where they felt most vulnerable to business disruption:

- 5 percent of the CFOs could not answer the question or did not know.
- 11 percent felt their firms were not vulnerable.

When asked if a disaster occurred that would definitely harm the firm's ability to continue, the CFOs felt that the areas where they were most vulnerable were as follows:

- 37 percent said vulnerable in disaster preparedness or a recovery plan
- 24 percent said vulnerable in the security of their information systems
- 11 percent said vulnerable in the protection of their intellectual capital
- 12 percent said vulnerable in their ability to detect fraud or employee theft

The Committee of Sponsoring Organizations of the Treadway Commission and ERM

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) recently issued its new framework titled *Enterprise Risk Management—Integrated Framework* (ERM framework). This framework builds upon the 1992 report that addressed auditing internal control. The ERM framework was written by PricewaterhouseCoopers on behalf of COSO. This guideline contains key concepts and components of effective risk management, such as philosophy, risk appetite, and viewing risk as a portfolio.

As finance managers, auditors, and consultants, we must recognize that our role includes providing assurance that controls are in place for detecting and monitoring problems. Both COSO's recent framework and Sarbanes-Oxley have created a new role for us:

The accountant is a key member of the firm's ERM team.

Because a significant business risk could arise from nearly every decision and action undertaken by the firm's employees, we need to be very aware of the causes and contributors to costly risk. Based upon my career spent analyzing risk and understanding leadership, I offer the following process view, especially for auditors. Auditors must understand ERM's impact on their clients because of both COSO and Sarbanes-Oxley requirements.

Exhibit 3-1
The ERM Self-Sustaining Cycle

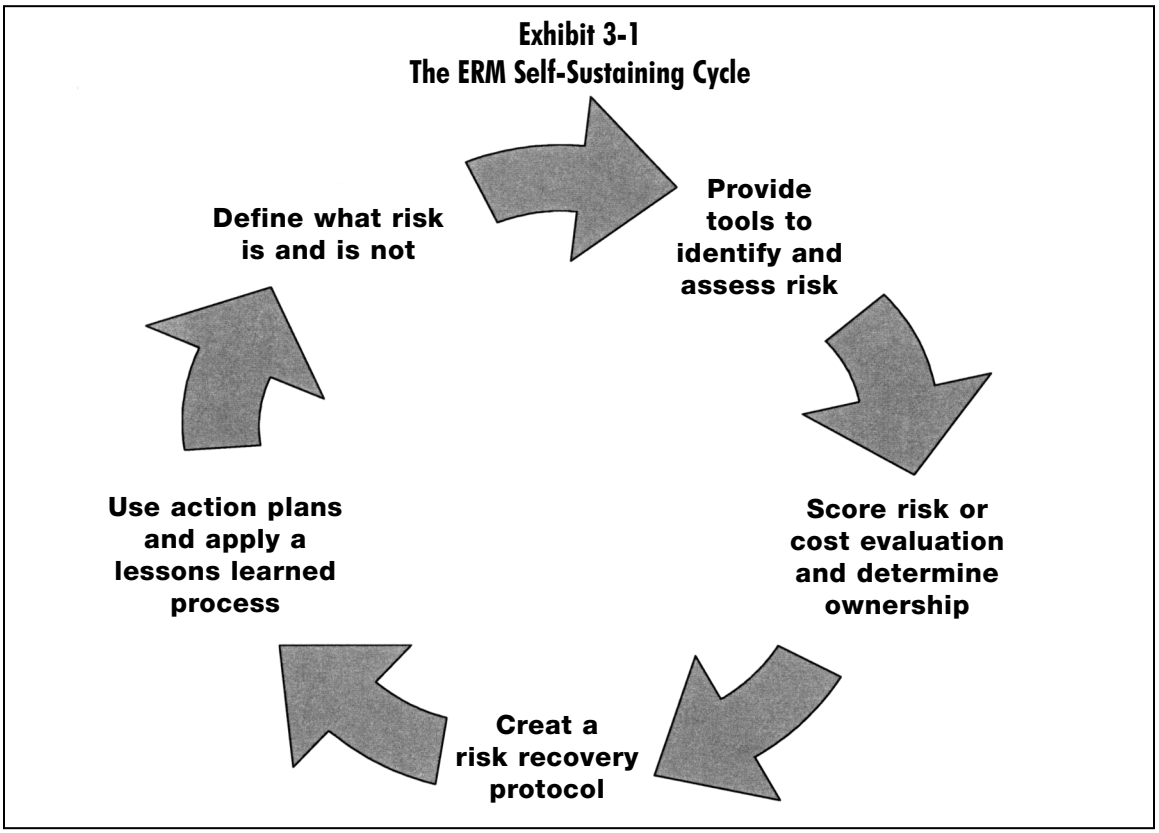


Exhibit 3-1 is a visual view of the ERM continuum. It starts with defining what risk is and what risk is not, then follows the path to the action of providing employees with tools so they can identify risk. From there, ERM requires using tools to do risk scoring and cost valuation, while ensuring that someone owns the responsibility for many managing the risk. The next two steps include employing a protocol for risk recovery and defining specific action plans for learning from the risks taken. Notice this continuum follows the six steps that we will be following in this book to create a risk and balanced culture.

5½ Myths of ERM

1. Myth: ERM is mostly about effective internal controls—financial and operational.
   Reality: ERM is about leadership, decision making, and justifying the risks we undertake.

2. Myth: Auditors and accountants are mostly responsible for applying ERM.
   Reality: Everyone in the firm is responsible for fostering and applying a risk management system.
3. Myth: If your ERM works, you will be assured that risks will not be costly or wasteful.
   Reality: The failure of a risk could still be costly, but ERM allows you to recover quickly and confidently and know that the rewards exceeded the costs.
4. Myth: ERM mostly addresses external risks, such as market and regulatory.
   Reality: Because risks can arise from anywhere and from multiple sources, ERM requires both an internal and external focus and awareness.
5. Myth: The best measurement of ERM's effectiveness is lower insurance and compliance costs.
   Reality: The primary measurement of ERM is adding value to the firm, as defined by the stakeholders.

5½. Myth: ERM only applies to big, for-profit companies.
   Reality: Every firm that faces risk can benefit from applying the fundamentals of ERM—it is necessary for survival.

ERM in a Nutshell

ERM enables leaders to deal with the uncertainty that harms firm value.

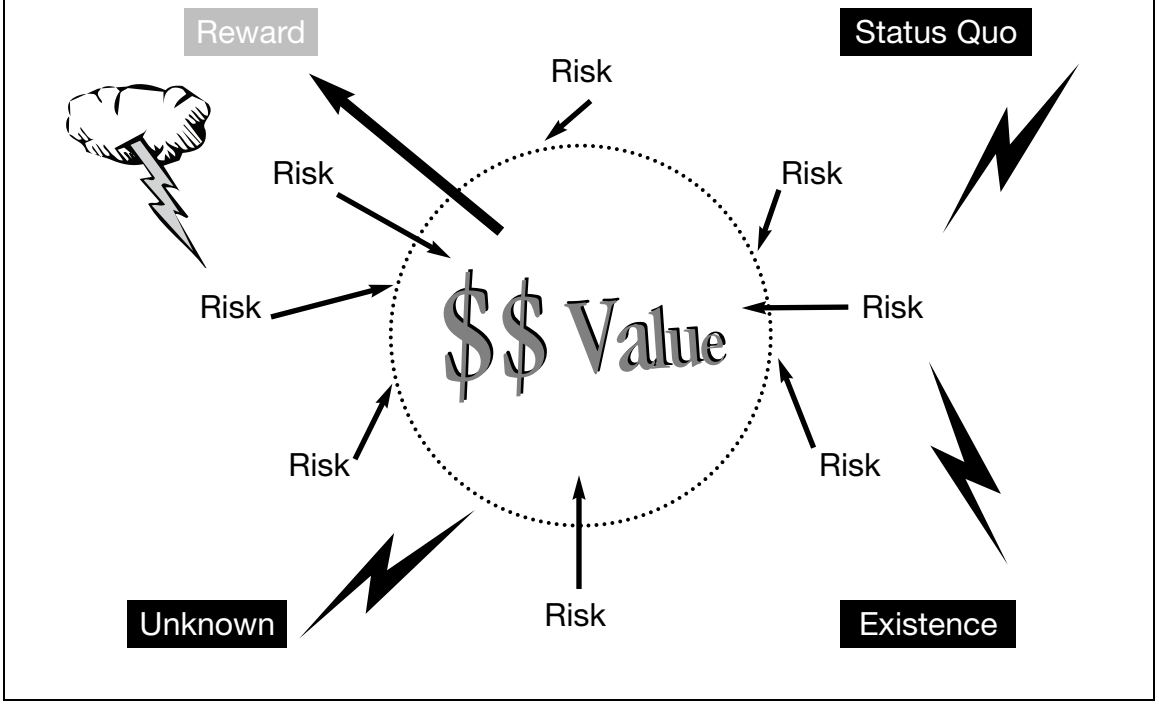
ERM represents a fundamental shift in the way businesses must approach everyday risk. As our economy becomes more service and technology driven and globally oriented, businesses cannot afford to let new, unforeseen areas of risk remain unidentified or ignored. We now have more guidance on the implementation of a consistent ERM framework with COSO's ERM framework. The framework strives to define and describe ERM and provides a standard against which businesses can assess their ERM program and determine how to improve it. This effort began in 1984 when COSO first addressed the issue of internal controls and inherent risks to respond to excessive frauds, scandals, and audit failures.

Lessons from M&M Candy

The M&M candy protective coating is one thing we all loved and enjoyed in our youth. In fact their catchphrase was, "Melts in your mouth, not in your hand."

As shown in exhibit 3-2, ERM provides a protective coating to the core, which is your firm's value. The entire organization is moving toward some sort of reward. All sorts of risks (lightning bolts) occur from many sources, such as the status quo, the unknown, and even just being in existence: risks that the firm is subject to that could harm firm value. Your ERM culture and methodology works to deflect, defer, and minimize most of the risks. Although some of the risks will break through this protective shell, the organization is strong enough to deal with those few risks that get past the ERM structure.

Exhibit 3-2
ERM Protects Firm Value



COSO Addresses Risk Management

Back in 1992, COSO issued its original framework on internal control environments. Even then, COSO was attempting to get our attention on the importance of addressing risk. From COSO's original report, we see the five interrelated elements of internal control:

1. *Control environment*—Integrity, ethical values, competence, management philosophy and operating style, authority and responsibility, and people development
2. *Risk assessment*—Identification, analysis, and objectives
3. *Control activity*—Policies, procedures, directives, and actions
4. *Information and communication*—Identification, capture, dissemination, action responsibility, and flow
5. *Monitoring*—Assessment of quality and measurements

Statement on Auditing Standards (SAS) No. 109

Current auditing and accounting pronouncements such as SAS 109 and the recently published Risk Assessment Standards have made it clear that auditors and management are responsible for identifying and addressing risk.

When I first entered accounting in 1979, the risk auditors addressed was mostly focused on misstatements that lead to an unreliable financial statement.

Because of sophisticated schemes to hide bad decisions and unaddressed risk (see Enron, WorldCom, et. al), every professional in accounting has been put on notice that unmanaged risk can lead to fraud.

How to Apply ERM

ERM is a very effective strategy that any firm can use to manage a wide variety of risks, running the gamut from strategic or financial risks to man-made or natural disasters. The difference between ERM and more traditional methods of managing risk is that ERM calls for high-level oversight of a company's entire risk portfolio rather than the silo or stovepipe approach. The outdated and ruinous silo method is built on the hope that individual managers alone will identify and oversee specific risks.

ERM centralizes all risk management under a chief risk officer position or a risk committee that supports the individual risk bearers to help each one of them identify how much risk the entire entity can tolerate, formulate mitigation strategies, and otherwise capture advantages of risk opportunities.

Risk requires absorbing, hedging, or transferring risk and applying capital to it—money that could be spent in other parts of the business. This view of throwing dollars at risk or the cost of ERM, in effect, helps the organization's leaders determine the right amount of capital that should be directed toward risk.

Proper risk management is done by gathering information from the various people overseeing risk areas and using the combined knowledge to determine the threats to the organization, their financial impact, and the effectiveness of the firm to handle such risk. The goal, of course, is to determine the appropriate amount of capital we need to protect ourselves from risk. The risk committee is the champion for the information gathering efforts.

Within the ERM structure or framework, the firm establishes a risk definition and the tolerance levels (the cost we cannot afford) as well as the policies and procedures required to assess and measure the risk and create systems for monitoring and detection. This is in line with step 1 of our six step process (chapter 5).

Example: Dashboard Approach

Most modern accounting software uses this technique in its reporting module. The report screen displays an actual dial showing goal achievement in three colors. The goal could be a budget target, standard, or performance metric.

Each dial provides the reader with immediate feedback on goal achievement. The dashboard format is an offshoot of the balanced scorecard approach to reporting and measuring.

Monitoring and Measuring Risk

ERM establishes a hierarchy of specific risk managers who report to the ERM executive and employs a dashboard approach. The scorecard software provides the business intelligence that extracts risk-based information, collates it, and provides it to the chief risk officer or ERM committee. This bird's-eye view of risk is not available with the traditional silo-managed risk methodology where we rely mostly on insurance to address hazard and liability risks. The ineffective silo or stove pipe approach does not work because

- internal audits only deal with control risks.
- finance only looks after financial disclosure and reporting risks.
- operational people only deal with day-to-day business risks.
- asset managers are only concerned with property risks.
- executives mostly deal with strategy risks.

- sales management only looks at market and customer risk.
- quality watches over product risk.
- treasury solely handles monetary risk.

Not only does it separate liability from the solutions, it also prevents communications about risk, the sharing of best practices, and risk trend analysis.

Risk Oversight Team

ERM requires that all members of the ERM committee work together to pinpoint and measure the critical risks confronting the organization and then develop a systematic approach to manage the risk portfolio.

Companies that attempt to manage their risks focus mostly on strategic risks and ignore such things as insurable risks.

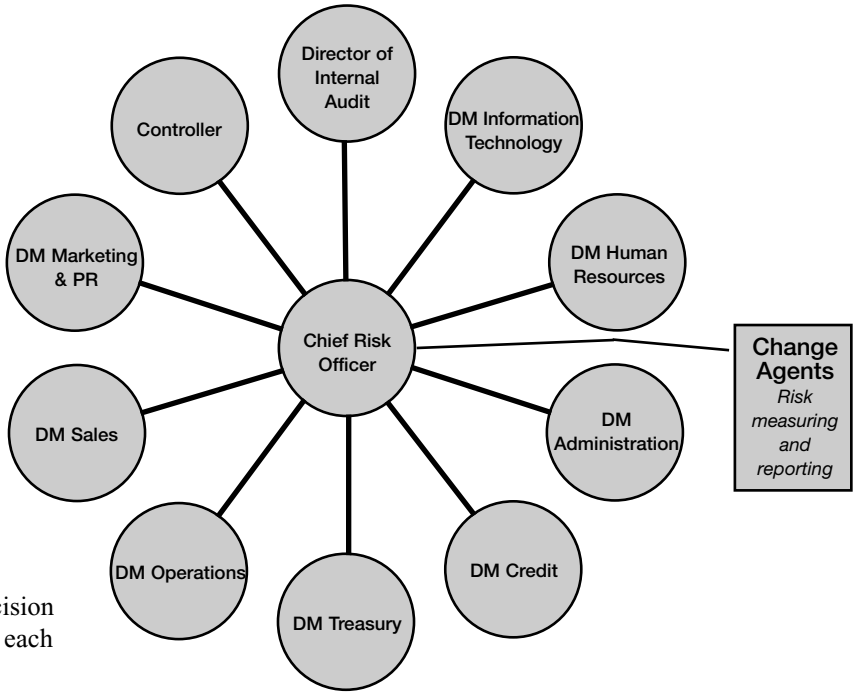
One best practice in ERM is a risk matrix. This tool allows the alignment of the risk and business processes to ensure that data relating to each risk is routinely stored in the database that is accessible by the CRO. A critical part of ERM rests on the correct collection and organization of data regarding potential risks. ERM relies on technology to determine and identify risk trends and provide feedback on the management of each risk. ERM needs to be viewed as a management function, a given for running the business better.

Bad Strategy Now in Vogue

Some organizations are using the internal audit department as the ERM implementation group and the chief auditor as the chief risk officer. This is not a good strategy because the sorts of risks auditors look for may be very different from the ones that could undermine the organization. Internal auditors tend to focus on processes and areas of financial risk. Yet the risk could occur from almost anywhere—from an employee's decision, to a manager's attitude, to a Web site transaction. To be able to comply with Sarbanes-Oxley, companies must be able to implement an ERM system within their organization because it calls for continuous monitoring and measuring of the organization's ability to face any risk.

As you can see in the risk management team's organization chart in exhibit 3-3, there are many participants on this team. Its membership consists of the controller and key decision makers from every part of the business—from HR to sales and from operations to treasury. The center or focal point of the team is the chief risk officer. I recommend that the CFO not be a member of the risk management team as a way of strengthening the checks and balances. The members of this team, other than the controller, need to be someone charged with responsibility for the quality of decisions and processes within the department that they represent. In a smaller organization, this person could be the actual department head. However, in larger organizations, this responsibility could be assigned to someone (other than the head) as a way of building the competence and confidence of that future leader.

Exhibit 3-3
Risk Management Team Membership



Includes a key decision maker (DM) from each functional area.

The employees that the chief risk officer supervises can be referred to as change agents. This title reflects more of what their ultimate goal is rather than their responsibility. Their job will be to

- look and delve into certain areas that are or will be affected by risk taking.
- assist in implementing the changes that the risk management team recommends.
- train employees on how to use the risk management tools.
- report to management with a balanced set of risk taking metrics.

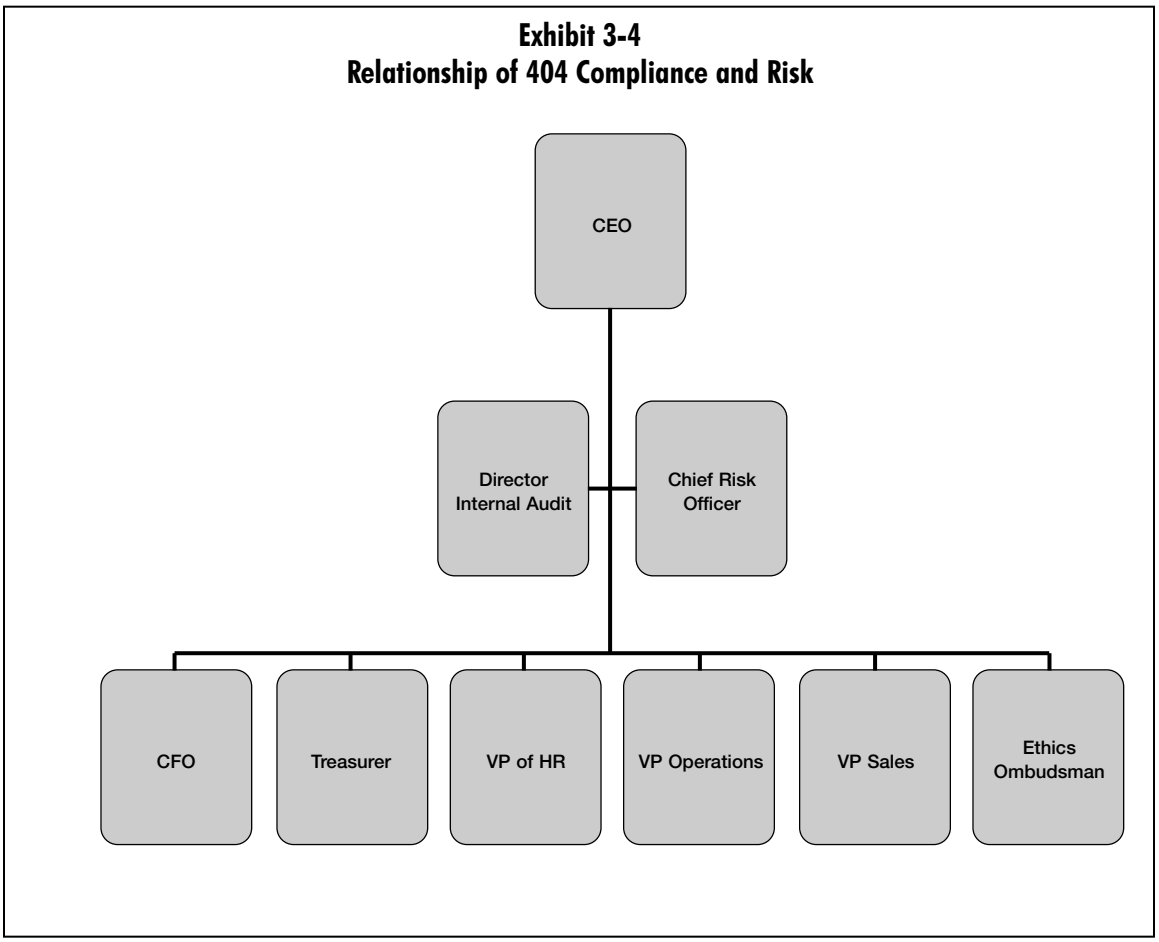
You could give other titles to the employees who report to the risk officer, but giving this employee a title such as analyst, auditor, or risk assessor does not communicate to others what they are doing for the organization and could be confusing if you have other employees with those titles.

Integrating Section 404 and Risk Compliance

If you are involved with implementing section 404 of Sarbanes-Oxley, a critical question that I am often asked is, "How do I integrate risk management into our Sarbanes-Oxley compliance program?"

If you look at the organization chart shown in exhibit 3-4, you will discover the answer. The internal audit function, led by the director of internal audit, is one of a set of conjoined twins. The other twin is the chief risk officer. The internal audit group focuses on problems that could lead to a faulty financial statement. The risk management team focuses on risks that could affect the bottom line and firm viability.

Exhibit 3-4
Relationship of 404 Compliance and Risk



Although both teams are concerned with breakdowns in internal controls, in faulty decisions, and in detecting people who are hiding problems, their primary focus is different.

The chief risk officer's team is charged with the concept of what is risky and what is not. They will be seeking out areas where the payoffs for risking are overstated or where the costs of risking are understated. These potential problems may or may not show up in assets or in specific transactions. This is where the internal audit team shines. They will be examining documentation, testing transactions, and reviewing specific accounts. Yet together, their combined view gives the CEO and the board of directors a fantastic window into what is occurring internally. The things each team looks at will also highlight external areas of concern. If both the leaders of internal audit and risk management give the CEO assurance that risk is being managed and the firm's checks and balances are working, the CEO can definitely sleep well at night.

By looking again at this flowchart diagram, you see that the chief risk officer and director of internal audit are independent from accounting and work for the CEO in a staff capacity. Please note that another key player in every risk management program and Section 404 compliance is your ethics ombudsman. Like the chief risk officer, this position is required by Sarbanes-Oxley. The ethics ombudsman is a line function that works under the CEO and reports directly to the board. This person and his or her team are concerned with compliance with the firm's code of ethical conduct, and the cultural norms that ensure people always take the ethical high road.

Another reason these two teams need to be installed at a high level with executive status is the urgency for implementation of positive improvement. The internal audit team will offer recommendations to oper-

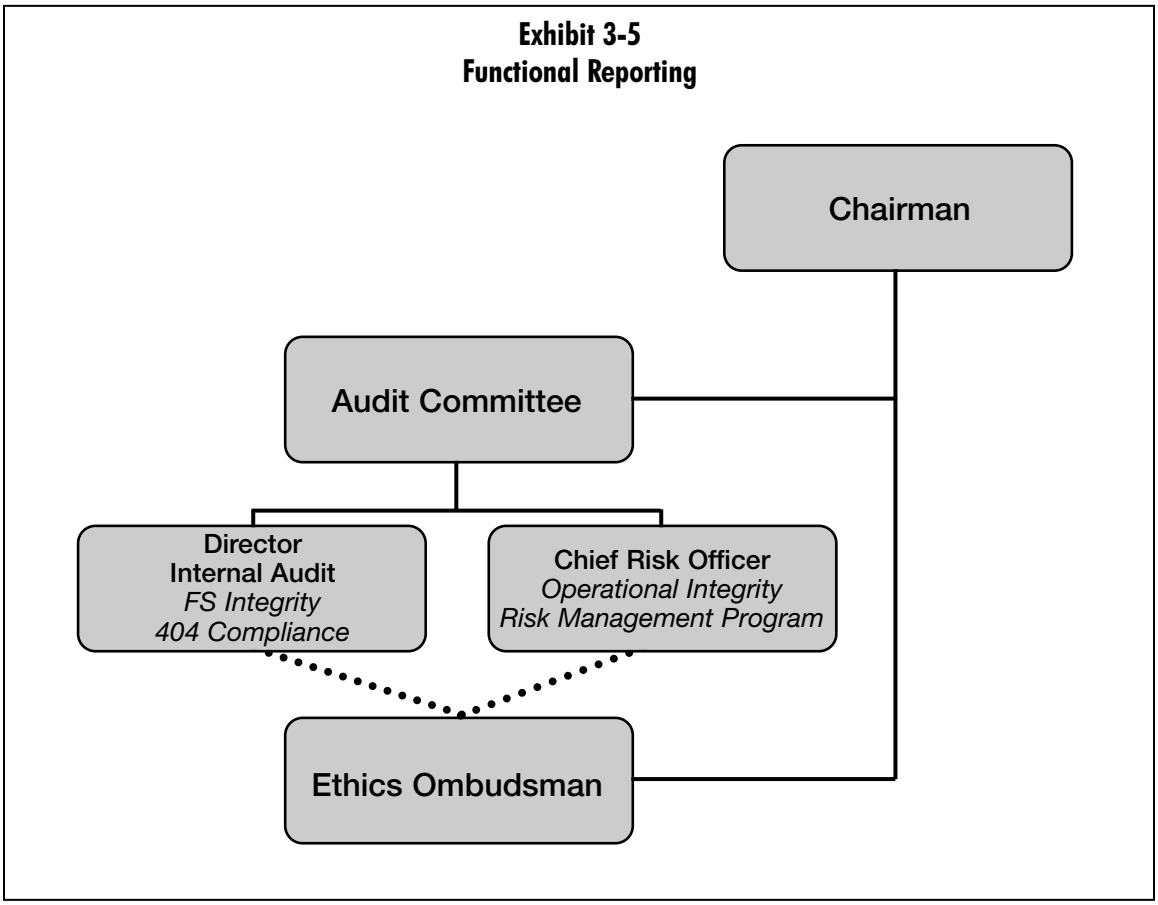
ational managers and others on improvements they feel will strengthen internal controls. Quite often, the internal audit team's recommendations are not taken seriously. When the same recommendations are made by the internal audit director's twin (the chief risk officer) the impetus for making the change grows exponentially. In addition, if the ethics ombudsman echoes the same concerns, the seriousness of the issue rockets up the charts!

Functional Reporting Responsibility

In exhibit 3-5, "Functional Reporting," you will notice that both positions report directly to the audit committee. As stated before, the director of internal audit is concerned with financial statement integrity and leading the Section 404 compliance efforts. The chief risk officer, on the other hand, is concerned with operational integrity and leading the risk management efforts. There will naturally be some overlap in their specific responsibilities but they both end up reporting to the group who has been charged, by the shareholders, with overseeing the financial and operational viability of the firm. Notice also that the ethics ombudsman is a third member of this compliance trilogy because what he or she learns in administering the ethics program will be reflected either in financial statement integrity or operational integrity. The ethics ombudsman also reports directly to the board's audit committee because this person has tremendous insight into areas at risk for fraud or mismanagement from the employee level.

As we have seen from the recent instances of fraud, the CEO and CFO were in collusion (Aldelphia), the CEO condoned the CFO's fraud (Enron), or the CFO was intimidated by the CEO (Worldcom). This functional reporting reduces the likelihood of these occurring within your organization.

Exhibit 3-5
Functional Reporting



Capital One's ERM Strategy

Capital One is a one hundred billion dollar financial services organization that uses ERM. Their ERM strategy is built on the belief that managing risks holistically offers value for identifying the breadth of organizational risks, quantifying them, and distinguishing their impact and correlation to one another.

Capital One uses an ERM team that sets the methodology and reporting standards, then educates employees about risk. They use their internal audit team to ensure that risk management processes actually work. They also have a Chief Risk Officer who heads the ERM efforts. The fourth group, included in their ERM structure, is the functional groups throughout the enterprise who actually manage the risks and report the results to the ERM team.

Capital One uses business intelligence software designed around dashboard technology that extracts risk-based information, collates it, and reports it to the Chief Risk Officer. When interviewed about their ERM process, Michael Glotz a Capital One Audit Director said, "Someone has to bring risk management into the strategic planning process to ensure business strategies are aligned with the organization's overall appetite for risk." This is how ERM works at Capital One.

Summary: Clear Payoff of ERM

Companies that incorporate ERM into their strategy achieve positive returns on their identifiable risks and help to stabilize their earnings by lowering the cost of capital. By employing the best practices and tight controls built into a risk management system, the company avoids the pain of people who color outside the lines too far or who underestimated the cost of a specific risk.

To avoid any negative outcome and promote shareholder confidence, the firm's leaders need to instill transparency to both investors and others inside and out regarding the risks that it is undertaking, especially those that will build, but also could harm, shareholder value. Incorporating a risk management program into your culture by following the six steps will result in managers being able to make this integrated risk disclosure:

> *"Management is 93 percent confident that earnings estimates will not deviate from the expectations by more than $10 million or 6 cents per share as a result of market risk."*

4

Your Firm's Risk Management Plan

You always get what you measure, so measure what you want to know.

After completing this chapter, you should

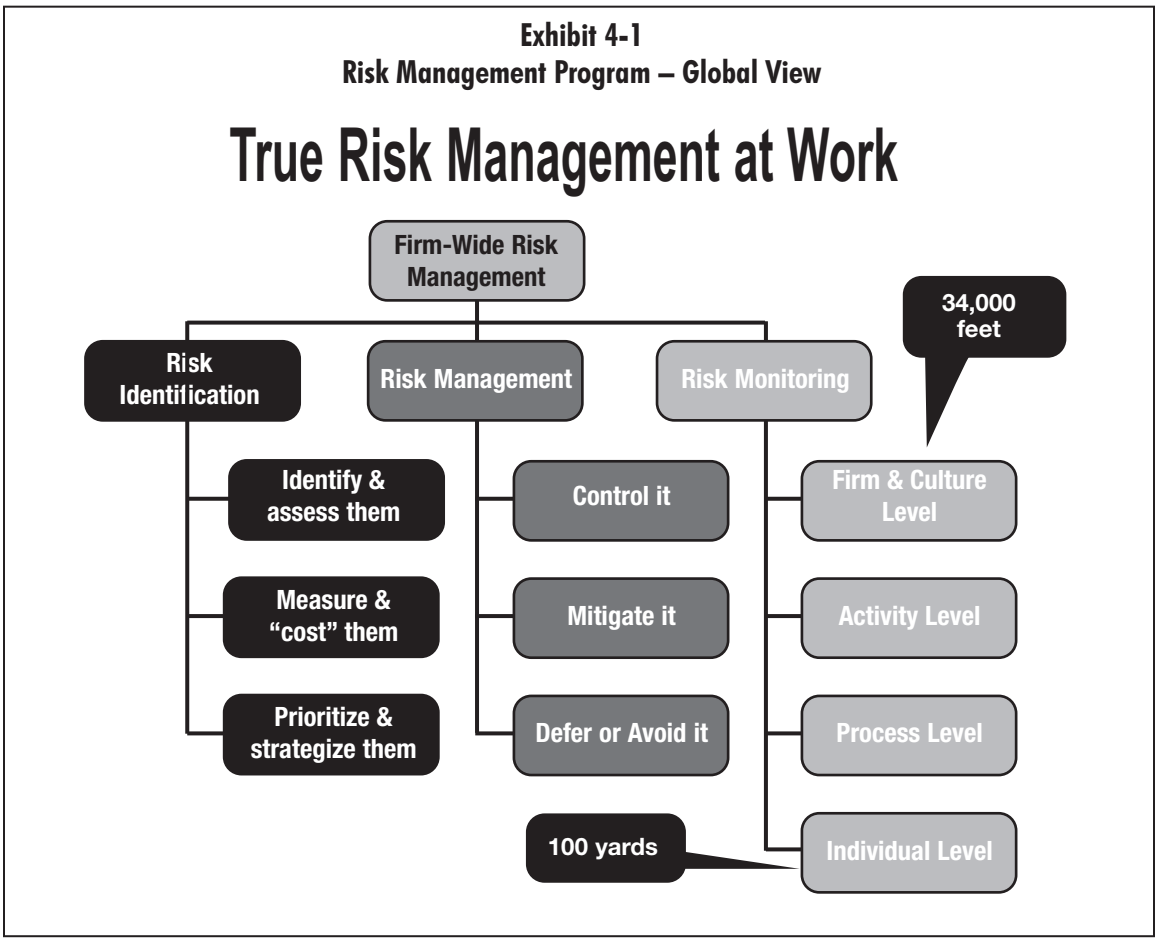
- understand why a firm needs a defined risk management program.
- see how to use your risk management plan to help prevent fraud.
- be able to identify who should be the risk champion for your organization.
- be able to help others foster a risk awareness in your organization.

Five Stages of Crisis Management

Stage 1: Denial
Stage 2: Containment
Stage 3: Shame mongering or the blame game
Stage 4: Blood on the floor
Stage 5: Solution (crisis gets fixed)

This describes most firms' process for handling risk. In fact most governments follow this process too! Nothing gets better because leaders get stuck at stages 3 and 4. Look at the handling of Hurricane Katrina, but that is a lesson for another time.

Exhibit 4-1
Risk Management Program – Global View



Your Risk Management Program

Every firm needs a defined risk management program! With one, your firm increases its longevity and profitability. Every day, things occur that could undermine the organization's success. Wouldn't it be better if people in your organization were better prepared to handle those unexpected events?

Assume that you took your family on vacation somewhere distant and failed to study the type of weather you would encounter. You might pack for sun, and it turns out to be cold. You might pack for outdoor activities and have to spend the entire vacation inside. This is what your risk management program is about: *matching your plans with the existing environment*.

In exhibit 4-1, a global firm-wide risk management program consists of three prongs or strategies:

1. The first strategy is identification of the specific risks. In this strategy, you identify and assess risks, measure them, and then use this information to prioritize and strategize each identified risk.
2. The second strategy is to arrive at specific ways of dealing with the risk, such as controlling it, mitigating it, or, better yet, avoiding it.
3. The third strategy is to monitor the risk. This is the most neglected strategy of the three because we have to slice and dice each identified risk in four different ways. We look at the potential risk at the macro level to determine its affect on the culture, at the individual level to see how employees view

and handle the risk at the process level, and, finally, at the activity level where the actual decision takes place.

If you have not been involved in a risk management program, you may notice it looks like a lot of work. It is! However, the payoff is tremendous. This chapter will focus on a few specific areas where you benefit from having a risk management program, including fraud, financial loss, information, strategy, and business operations. Before completing this chapter, you will understand why every firm must raise the level of risk awareness.

Fraud and Risk Management

Risk Awareness Prevents Fraud

Almost every business leader believes that only people with high ethical standards work for them. Yet, research shows that 30 percent of today's workers are always looking out for ways to steal from their employers and another 30 percent will steal if given the opportunity. Fraud is most likely to occur when an employee serves as the sole contact with a particular vendor or when one person performs several incompatible functions. Once fraud schemes begin, they are hard to detect and even harder to stop.

There is clear evidence of fraud right in front of you, but you need to know where to look. Awareness begins by

- analyzing patterns.
- looking for photocopied or altered forms.
- analyzing credit invoices for excessive activity or unusual patterns.
- checking that the vendor was properly approved.
- looking for complaints from outsiders and from employees.
- conducting address checks and site visits more often.

Detecting fraud is difficult even for professional investigators. The best option is to concentrate mostly on prevention. So having a risk management program in place forces leaders to seek out areas that are at risk. Areas open to fraudulent activity will be easily uncovered.

Profits and Risk Management

Risk of Financial Loss

A 1999 survey of Fortune 1,000 companies, conducted by Mercer Management Consulting, found that 10 percent of those companies suffered a 25 percent or greater loss in shareholder value during a single month period between June 1993 and May 1998.

The sources of the losses came from

- strategic risk—58 percent suffered a drop in stock value and traced it back to competitive pressures and revenue shortfalls.
- operational risks—31 percent of the losses.
- financial risks—11 percent of the losses.
- hazard risks—no losses were reported because they (usually) had insurance to cover the losses.

This information tells us that there are other areas at risk and that is where leaders need to be watching. These areas can significantly affect the financial success of the organization.

On-Spot Information Gives Rise to Profit Potential

Firm-wide risk management allows organizations to examine all the risks that they potentially face and to measure the impact of those risks on the organization. Firm-wide risk management also helps firms identify appropriate steps to manage or mitigate those risks. The risks businesses face include, but are not limited to, hazard risks, such as property damage and theft; financial risks, such as interest rate and foreign currency exchange; operational risks, such as supply chain problems or cost mismanagement; and strategic risks, such as misaligned products or overly aggressive strategies. The key to your program is to address all those risks in an integrated fashion.

The reason that a risk management program protects profits is due to the process of identifying, quantifying, and prioritizing risks, making them more real and visible to leaders who normally fail to give risk management the attention it deserves. Another reason is that a firm-wide awareness requires a holistic approach to risk management beyond the traditional parameters of things that are insurable. This cultural discipline greatly expands the company's definition of risk to include anything that threatens the organization's continuity. A companywide approach helps the firm to sort risks into those that can help the company grow and those that will only lead to loss. In the rush of global competition, sometimes this differentiation is not easy to spot.

The aspect of identifying, quantifying, and managing all the risks that a company could face is compelling but daunting. For any risk management program to be effective (enterprise risk management [ERM]-based or not), your organization must clearly define its goals, make them realistic, and identify their intended results. The end results will both adequately protect the organization and allow you to identify opportunities to grow, expand, and gain shareholder value. Because it would be nearly impossible for the company to quantify every risk it faces, risk identification starts at the "34,000-foot level" (see chapter 3). Later in the process, you will empower employees to deal with risks at the close-up or "100-yard level."

The Risk Champion and Risk Team

Every risk management program (ERM-based or not) requires a senior level champion. This champion must be able to assemble a multidisciplinary or cross-functional team that can effectively discuss the risk and the related business issues that the company faces and then share those findings with the entire organization. Of course, your risk management program must have the support of the board of directors because your risk committee requires representation from all across the company and is necessary to create stronger ties between the oversight of risk and the application of the tools and mitigation of the risks. It will be the ultimate responsibility of line managers—risk takers—to be able to identify, classify, monitor, and control operational risks. Unfortunately, without the risk management program, most organizations assign their risk management to either a professional risk manager or to their CFO. The champion for risk awareness-the chief risk officer-and the risk team must take the time to understand why the company has succeeded in the past and is currently succeeding or not succeeding.

The biggest challenge of a risk management program is to bring the company to a point where it can identify the risks that are the greatest threat to its continued growth and success, quantify the size of those risks, and, then, take steps to manage or mitigate them. Although most businesses that currently use ERM initially identify between 50 to 100 or more specific risks, the key is to narrow it down to the top 5 or 10 risks that are significant enough to warrant quantifying and analyzing. Once a company has identified its key risks—among those top 10—it has to quantify the magnitude of those risks. Quantification helps the leaders to decide whether to control, prevent, finance, insure, or avoid the risk altogether.

In the event that a risk needs insurance, your company still needs to take a fresh approach. While adopting specialized insurance approaches, your organization needs to work toward long-term solutions. For example, a risk to your firm's brand might be easily mitigated currently, but in the long run it could have a significant negative impact on the marketplace if not addressed today. Brand risk is an example of an exposure that may not be covered by your current insurance coverage. This is why your recovery plan is critical to the successful implementation of risk management. Throughout the entire risk management process, companies must retain a strategic focus. This is another reason why a senior level executive must be the champion of your RM efforts.

Your Business Plan Risk

A company's business model is made up of two components:

1. The organizational structure and processes
2. The impact on operational risk from decisions made

In addition, if an organization is unable to perform or execute its strategy, the firm incurs execution risk. To assess and measure execution risk, a company focuses on the results it generates from the structure of its marketplace and its business model. Within the theory of your business model, three specific global risks reside:

1. Strategic risk
2. Operational risk
3. Innovation risk

Strategic Risk

Strategic risk is defined as the inability to align with competitive pressures and customer sufficiency. Falling under the threat that you cannot carry out your strategy are eight risk categories:

1. Operational risks (execution of your strategy and goals)
2. Reputation risks (impact on your reputation and brand)
3. Financial risks
4. Hazard risks
5. E-commerce and technology risks
6. Intellectual capital risks
7. Ethical risks
8. Integrity risks

Risky Strategy Leads to Ethical Risk

Strategic planning is managing change and overcoming risks. It is a critical process where risks can and need to be identified and dealt with in advance.

For your firm to manage your strategy risk, the leaders must develop acceptable expectations for all products or services. A risk to your firm's ethical standards is involved here, because there is intense pressure on the organization and the employees to meet a lofty goal, to achieve its business plan, and to satisfy creditors or investors. The more this pressure is applied, the more likely people will undertake unwarranted risk. If these wild, out-of-control leaps fail or do not achieve the high expectations, there is urgency for people to cover them up. Thus, your integrity is at risk.

Risky Market Leads to Integrity Risk

In market risk, firm integrity is involved and can be damaged when your research or studies are flawed or when your assumption of the customer's needs is skewed in favor of the organization. Many market studies have been accepted as true without consideration of the realities of the market place or not obtaining true customer buy-in. Facing this risk requires you to get your input about the competitive environment from the source.

Risky Capability Leads to Integrity Risk

The capability or internal risk is another place where extreme pressure is felt when it is clear you will not achieve your goals. It is important to challenge people's ability and to test their capability to grow, expand, and improve. However, leader hubris combined with undue pressure is often applied when you over-promised and must now under-deliver. People will want to massage the numbers, to make up data, and of course, to hide the internal faults. This last trait leads to buck-passing and blaming. These, of course, negatively affect the profits and damage integrity. The net result is bad news for all!

Operational Risk

Operational risk management looks at the business from the operation itself and is defined as the risk of direct or indirect loss resulting from inadequate internal control, processes, people, and systems to react to external events. Financial information is not enough to gauge a company's overall business risk.

The value of managing operational risk is only slowly gaining recognition. One reason is that by the time financial impact for management's misjudgment affects the balance sheet or income statement, it is usually too late to do anything about it other than pick up the pieces. By tracking operational indicators and metrics, leaders can identify opportunities and threats *before* they affect the company's finances.

One approach to measuring operational risk requires firms to routinely review many nonfinancial factors such as the quality of corporate governance, employee morale, customer satisfaction, implementation of goals and execution of those goals, the company's application of technology, and its deployment of those practices. Numerous tools that enable you to easily measure operational risk already exist, such as the balanced scorecard, activity-based costing, or driver-based forecasting.

Budgeting Hampers Operational Risk Identification

Most companies still rely on their planning and budgeting process and historical reporting techniques created in the 1930s. To improve the likelihood of detecting operational risk, organizations can do the following:

- Update their technology
- Use advanced analysis tools
- Apply for ISO 9000
- Qualify for the Malcolm Baldridge Award
- Use a balanced scorecard reporting system
- Incorporate activity based costing
- Invest in an enterprise-wide accounting system

Managing operational risk requires a systematic, objective, and comprehensive framework that assesses all of the nonfinancial variables that could contribute to an organization's risk portfolio.

All firms incur certain operational risk simply when choosing their marketplace and its customer base. Business complexity and revenue volatility are directly affected by the structure of the market. Technology, regulations, the consumer, and the global economy all drive changes in market structure. All of these must be factored into the assessment and valuation of your operational risk.

Key Drivers of Operational Risk in Your Market Structure

- Number of participants
- Degree of concentration
- Level of regulation
- Competitive environment
- Rate of business growth
- Capital intensity
- Barriers to entry
- Product life cycles
- Availability of alternative markets
- Risk of obsolescence

Key Drivers of Risk in Your Business Model

- Governance model
- Organizational structure
- Product or service delivery model
- Process complexity
- Technology complexity
- Sourcing strategy
- Best practices utilization
- Management discipline
- Staffing and employee skills
- Leadership competency

Key Drivers of Risk in Your Execution Efficiency

- Revenues
- Earnings
- Cycle times
- Growth
- Quality
- Service levels
- Productivity
- Market position or market share
- Management competency

Key to Measuring Operational Risk

The starting point to measuring operational risk is to make sure you are collecting the right data. This requires a complete and balanced view of your key business metrics across at least three dimensions and must include a mix of leading and lagging indicators. Your operational data must be able to describe how a key operation is conducted within your organization.

To overcome any information deficiency, your organization must effectively combine operational and financial data together in order to form a more complete and timely picture of operational risk, while decreasing your reliance on historical financial reports. Your leaders need to assemble a list of possible and predictive metrics for the business and then test them to make sure that they correlate the time lag of the activity indicator to the time of its financial impact. The ultimate payoff is that you can use these operational risk metrics as targets for your budgeting process. Thus, your budgeting process strengthens.

Regularly assessing your firm's operational risk profile benefits the shareholders. Of course, leaders and the employees of the organization grow in their ability to both spot and manage risks, and, most importantly, convert them into opportunities. Understanding your risk profile is a benefit to your customers and suppliers as well. This insight gives your leaders clues into areas that offer the best benefit for allocating resources and making tough decisions.

Effective operational risk management has gone from an "I would like to do" attitude to a "We must do this" frame of mind.

Innovation Risk

Companies undertake three sources of risks when they believe themselves to be innovative and desire a culture where employees think for themselves. In a culture of innovation and creativity:

- Innovation Risk Source No. 1 is the strategy risk. This requires clear direction setting and involvement to help the entire organization know where it is going and have the ability to measure progress.
- Innovation Risk Source No. 2 is market risk. This is the fear that the company fails to be in touch with the customer's needs and demands.
- Innovation Risk Source No. 3 is capability risk. This is a fear that the company will not be able to execute carefully designed plans and use the innovation to generate revenues.

Practical Solutions for Managing Business Model Risk

Strategy

The solution to making your firm less vulnerable is for your leaders to clearly define each of the firm's risks though your risk management program. It is particularly important to identify strategy risks early. This involves a matching of the role or purpose of your innovation with a specific strategic need for each new and existing initiative. Without such guidelines, new products, new ideas, and new services will misfire.

Market

For market risk, you need to prevent the risk that the innovation will not meet your market's needs. You need to ensure that you differentiate yourself from your competition or position yourself differently from what everybody else is doing. Because market risk is harder to measure and monitor, companies usually end up paying less attention to this risk. The number one reason for new product failure today is the inability to compete in both the global marketplace and on Main Street.

Operations

To minimize the operational risk, such as insufficient internal capability to deliver what you promised, or that your new product will not be developed within the desired time and budget, requires foresight and honest self-assessments. Defining your innovation risk up front will allow you to take the critical first step toward successfully managing it.

Innovation

All too often, leaders' expectations for new products go largely unspoken. They are in someone's mind, but frequently not communicated adequately to others. Most importantly of all, there is no way to measure

innovation and creativity. To help manage this risk more effectively, you need to develop and explicitly publish agreed upon expectations for any and all of your innovations. This process involves coordination of three separate and related tactics that allow you to effectively gauge how much risk you can afford to take.

10½ Rules for Successful Business Risk Taking

1. Focus on trouble, and you will get trouble. Focus on success, and you will get success.
2. Trust that your people know what a risk is.
3. Recognize that your people may not know how to recover from the negative effects of a risk.
4. No risk is worth undertaking when proper planning or analyzing cannot be completed beforehand.
5. No risk is worth undertaking when a "lessons learned" cannot be completed afterwards.
6. Every plan of action and strategy must have a feedback instrument built into it.
7. Understand the costs of your risk tolerance and your risk avoidance.
8. No one is exempt from making errors in judgment.
9. Tell the truth about the risk and its implications. Accept the truth about the risk and its implications.
10. Be willing to live with the negative results of each risk undertaken.

10½. Want more rewards? Take more risks! Want more success? Reward risk taking!

Answer this question:

What are these rules telling you about risk and risk taking?

Summary: Risk Requires a Proactive Plan

Global perils can come from any place within the business model, your strategy, or a new marketplace. Each one can deeply affect your firm's

- profits.
- creativity.
- continuity.
- brand or reputation.
- leaders' integrity.
- employees' ethics.
- internal capabilities.
- goal execution.

This is why the firm-wide plan for anticipating and dealing with these risks must become part of your everyday managing and leading.

5

Step One—Define Risk

The first step is always the hardest.

After completing this chapter, you should

- be able to test your definition of what risk is with others.
- understand why the firm's leaders must establish the corporate definition of *what is risk* every year.
- recognize the limitations of trying to purchase insurance to cover every risk.

There is a saying that goes, "Talking about bulls is not the same as being in the bull ring!" Therefore, we must grab the bull by the horns and face the situation! This, in essence, is step 1.

Exercise: Defining Risk

1. Write down the phrases or terminology you would use to define the word risk.
   Risk is ...
2. Write down the phrases or terminology you would use to define risk taking.
   Risk taking is ...
3. Next, ask a friend or colleague to define his or her definition of risk and compare your definitions. You will see that there is some terminology that is similar and some that is different. Write down any similarities you see.

The point of this exercise is to demonstrate that there are numerous ways for people and professionals to see and define risk.

The goal is to jump-start the process of gaining a consensus on a commonly acceptable definition of what is risky and what is the cost we cannot afford.

How others define *risk* (the most common answers): *Risk is …*

- "Doing something different."
- "Going outside of my comfort zone."
- "Scary."
- "Worth the effort."

- "Something that has an upside and a downside."
- "Putting something valuable on the line that I could lose or be harmed."
- "The unknown or X-factor."
- "Where I could get hurt or harmed."
- "A goal or destination that may not be achievable but is worth trying for."
- "A means to an end—hopefully rewarding or beneficial."
- "A movement forward despite any downside."
- "A gamble."

How others define *risk taking* (the most common answers): *Risk taking is …*

- "Going into the unknown."
- "Doing something proactive."
- "Having to face up to a potential loss or gain."
- "Going for something that has a payoff and a possible downside."
- "Doing a cost benefit ratio and proceeding with the assumption that the benefit is higher."
- "Putting something valuable at risk, often things other than money."
- "Taking a chance."
- "Pushing the envelope on what may not be acceptable."
- "Scary or frightening."
- "Not taking a chance."
- "Striving for some prize that may not be easy or even attainable."
- "Gambling."

Taking the First Step

What is required in step 1 of your risk management program is for the leaders and key decision makers of your company to sit down once a year and examine risk. At this offsite meeting, they dispassionately define, for the organization, what is considered risk taking and what are the costs they cannot afford. Over the life of the organization, this definition will change dramatically.

What You Will Discover In Step 1

By going through this exercise of examining different people's views of both risk and risk taking, you will discover a wide variety of definitions. The opinions will range from the optimistic to the pessimistic. Some people will focus on the upside or payoff (*worth the effort*) and others will focus on the downside or pain (*where I could get hurt or harmed*). Others will give you a balanced response, such as: *"Something that has an upside and a downside."*

When you compare all the various answers you will see a trend of three to five similar responses. Do not get hung up on the specific wording, but, instead, focus on the message behind the words. Your goal in step 1 is to get the group to arrive at a consensus on a mutually acceptable definition for both *risk* and *risk taking*. Based upon my experience, the consensus will almost always be the balanced views. I am always amazed at how pessimistic accountants tend to be when discussing risk. Likewise, I am also never surprised when marketing people and executives see risk as something necessary as they look through rose-colored glasses.

If your organization fails to take this first critical step in implementing a risk management program, you will find that people will take on more or fewer risks than they should. Employees will focus only on either the upside or downside of a risk. Some employees will ignore or overlook activities or decisions that contain risk, while others will over-dramatize the odds of failure.

Why Defining Risk Is Necessary

Because of recent changes in the world of corporate governance, boards of directors and other stakeholders of corporations are more wary of risk. To ensure their own job security, CEOs must become more aware of the need to develop more sophisticated means to measure and manage everyday business risks. Numerous experts agree that there is far less tolerance by stakeholders (especially in public organizations) for the executives who fail to prepare for a disaster of some sort. This leaves boards, shareholders, and executives searching for broader and better ways to manage risk in order to achieve their goals and ensure strategy viability. Thus, the entire organization must focus on the causes of risk instead of the traditional method of treating only the symptoms or focusing on the protection through insurance.

Operational risk management (as defined earlier) is managing the risk of loss resulting from

- inadequate or failed processes or systems.
- human factors.
- external events.

Operational risk management requires clearly defined authority and accountability for each sort of identified risk.

Practical Solutions for Making People Aware That Risk Exists

Simple Solution One

Share best practices across your organization. For this to occur, your culture must be one of openness, with managers as codependent partners within the risk environment. This partnership must include employees from the operational side of the business and employees whose advice is normally ignored such as the audit, finance, human resource, and risk management teams.

Simple Solution Two

Implement a governance structure. This is an integral part of the firm's operational risk program. Governance promotes cultural transparency and openness together with demanding accountability from each employee, each operating unit, and every support function.

Simple Solution Three

Identify, collect, and monitor a balanced set of key performance indicators or metrics that help the leaders to identify control issues and allow for early mitigation. This is also critical to operational risk management.

Case Study Analysis of Washington Mutual's Evolving Risk Appetite

Washington Mutual (WaMu) started out as a Washington-based savings bank. Then, as competition began to sweep through the banking industry and laws regarding ownership were revised or repealed, WaMu went from a button-down bank to an aggressive lender in the real estate marketplace.

In 1999, WaMu entered into a risky area known as subprime lending, competing with specialty lenders such as Ditech.com, Household Finance, and The Money Store. Investing in the subprime market is controversial because of the risks it poses for lenders due to the low quality of the debt and the higher interest rates that the buyers pay. WaMu Chairman and CEO, Kerry Killinger, justifies the risk this way: "We want-

ed to become a major player there to make sure subprime borrowers are handled in a fair and appropriate way." Mr. Killinger wanted the subprime part of WaMu to grow faster than its traditional mortgage lending. "We earn better margins in the subprime business because we're very efficient and have an advantage over some competitors," Kerry reported. It is estimated that about 10 percent of the loans that WaMu has in its portfolio are considered subprime.

More recently, they acquired a major credit card provider. WaMu, the largest savings and loan institution in the U.S. with total assets of $308 billion, expanded into the credit card business by buying Providian Financial, a once-troubled lender that bounced back from the brink of failure to become a prime takeover target. The combined company will have gross income of over $18 billion. With most of its profits tied to home lending, Washington Mutual is counting on credit cards to diversify its revenue as it strives to become more like a bank than a traditional savings and loan institution. They plan to use Providian as a springboard into the $800 billion credit card industry after the deal closed. "We view this as a favorable and transformational opportunity for Washington Mutual," Mr. Killinger stated in the acquisition announcement. He believes profits could rise even higher, if the two companies successfully sell more products to each other's customers.

WaMu was preparing to launch its own credit card before concluding it made more sense to buy the expertise and existing customer base of a major lender like Providian, which ranks among the 10 largest issuers with 9.4 million accountholders and $18 billion in outstanding loans. In a move to mitigate its risk and to thwart potential rivals bidding on Providian, Washington Mutual imposed a $245 million breakup fee as part of its agreement with Providian.

Providian Chairman Joseph Saunders, an industry veteran, is also a risk taker like Killinger. The Providian management team led by Saunders engineered a dramatic turnaround, which began in 2001, as the company battled to survive heavy losses that piled up from the company's former specialty of issuing credit cards to risky borrowers. "We took a significant risk to go to work for Providian and we did our job," Mr. Saunders said of his management team. The prior management team took on a risk that failed, while the current team took one that succeeded.

The 2006 acquisitions of both Providian Financial and MBNA come at a time when American banks felt the pressure to develop their higher-yield businesses, such as credit cards, while mortgage operations suffer from flattening yields thereby increasing their exposure. The question to be decided will be: is bigger always safer?

Looking at Washington Mutual's mission and values, we can gain insight concerning why the bank diversified its risk portfolio into credit cards and subprime mortgage lending.

What WaMu Values

"Vision: To be the nation's leading retailer of financial services for consumers and small businesses"

"Mission: To build strong, profitable relationships with a broad spectrum of consumers and businesses"

"We will do this by delivering products and services that offer great value and friendly service, and by adhering to our core values of being fair, caring, human, dynamic, and driven."

Values: [*an extract from their entire statement*]
"We are never satisfied with the status quo and know that we must continually reinvent our organization and ourselves."
"We continuously drive operational excellence to innovate our products, processes and services."
"We are committed to excellence and the achievement of superior long-term returns for our shareholders."
"We set high, measurable goals and hold ourselves accountable to achieve them."

As you can see, WaMu's values of

- "never satisfied with the status quo and ... must continually reinvent ourselves;
- [a] drive ... to innovate our products, processes and services;
- committed to ... the achievement of superior long-term returns; [set] high, measurable goals ..." gave the leaders carte blanche to be aggressive in taking risks. However, it has not always been this way. When WaMu first started, they were considered conservative and risk averse, investing only in high quality mortgages, which they serviced themselves. Back then, WaMu's leaders would not have considered (assuming the existing banking laws allowed them to) issuing a credit card.

Recent Updates

In 2005 and 2006, Wall Street rewarded WaMu for its risk taking by valuing the stock highly. As of 2007, Wall Street was punishing WaMu for its risk taking.

Apparently, the cost of these risks far exceeded the benefits. In July 2008, WaMu reported the biggest quarterly loss in its history: $3.3 billion in the second quarter. The bank has been adding to its loss reserves at a furious pace. This quarterly loss was their third in a row, each one totaling more than $1 billion. The losses from real estate mortgage financing will range between $12 and $19 million over the next few years, according to Washington Mutual executives.

Other costs WaMu could not afford include:

- having to immediately reduce more than $10 billion in operating expenses,
- getting out of the subprime lending business, and
- having to infuse new capital thus diluting existing shareholders' equity.

The risks WaMu undertook, focusing solely on the upside of higher than average returns and rapid growth, have come back to undermine their finances and reputation. I anticipate and will not be surprised if Mr. Killinger is asked to step down in the near future.

Answer this question:

Do you understand why your leaders need to review risk annually?

Insurance's Inadequacy in Risk Management

The insurance industry is only now beginning to address and work with their clients to deal with the risks in today's electronic world. Every day insurers are finding different exposures that they had not encountered before. The major stumbling block with insurers is the lack of historical data. Insurance companies use history to determine both the size of the risk and its statistical probability. From this data, the insurer sets a rate to charge its clients. This information must be reliable and always arrives years after the risk is identified!

In today's e-commerce, a lot of the risks are unquantifiable. For example, your business model requires a heavy dependency on a contract manufacturer. You are unaware that the contract manufacturer also consults with your competitor, causing your business harm. They failed to disclose this to you. You have to find and engage another contractor. You ask your insurance company for compensation, and they ask you, "What are your economic losses?" You are unable to show specific out-of-pocket costs other than some travel and legal fees. You argue for the loss of face to your customers and damage to your reputation for the effort in having to scramble to find an alternative supplier, and for lost future earnings. But because this is a contractual relationship and one not addressed in your policy, the chances are your insurance company will not reimburse you beyond your out-of-pocket costs.

This is a real risk facing every business that currently relies on strategic partnerships. In a panel discussion with top insurance experts, sponsored by the Risk and Insurance Management Society, this specific shortcoming came up. Both the representatives from the insurance industry and their clients expressed concerns that the insurance industry has been slow to see the need to assess and underwrite risk differently from its traditional methods.

The phenomenal growth in electronic business or e-commerce is another major and hard-to-quantify risk in business today. Although awareness to this risk is rising, some insurance companies still have a hard time getting senior insurance executives to recognize that this exposure requires a new strategy or approach.

Uninsurable E-Commerce Risk

All companies that pursue a business based around technology need to rethink their risk management processes. For example, when a software application in use becomes critical to your business and when organizations undertake business-to-business integration, the risk increases significantly. Your risk exposure grows because your partners can connect to your core data system. The exposure grows because your critical applications are operating 24/7, which increases the likelihood that someone may tamper with your systems. A disruption in business due to a virus or an electrical blackout could significantly affect your firm's financial performance. The potential losses associated with system malfunctions can manifest themselves in multiple ways, such as the loss of income due to business interruption, investor reaction that hurts share price, and the loss of trust in the integrity and reliability of your information system and Web site.

For the business that relies heavily on technology to be effective for your needs, insurance policies must underwrite your losses according to the decline in economic value of damaged property, whether it is proprietary information or intellectual property. As more losses include intellectual property thefts, companies need to ensure they have adequate internal protections. A key part of your risk management program needs to address intellectual property issues. Knowledgeable workers with access to a company's proprietary information may not know that they are misusing that information.

Uninsurable Risk of Doing Business Across the Globe

Another hard to quantify, yet uninsurable risk, is doing business globally. Even though you may not invest in bricks and mortar in a foreign country but are simply building a distribution channel or a base of operations to provide business services, you must closely examine the inherent risks associated with those activities. Be sure to develop specific cost-effective plans to address exposures, such as regulatory compliance, indemnity, currency and commodity price fluctuations, as well as employee or contractor safety.

What It All Means

No matter what new business risks are on the horizon or ones that have yet to have a label applied to them, a business leader's main concern needs to be:

How do we adequately overcome these risks with our own risk management program, especially when insurance coverage is inadequate or unavailable?

Fostering Risk Awareness Case Studies

Analysis of J.A. Jones Risk Awareness Program

J.A. Jones Inc. is a $3 billion global diversified services company. The company is attempting to create a tool for ongoing management, measurement, and monitoring of risk that can be used across all levels of the organization. It has been working on the tool for more than three years.

The CEO, Al Neffgen, set the strategy in motion with this goal: the creation of a centralized risk management process that could be coordinated with technical experts in all areas of the company. Another goal he set was to have the ability to educate and quantify key risks for business decisions, especially for capital allocations. The company wants to find the best way to monitor each risk and reward relationship. As its third goal, the company wants to integrate this tool in the decision makers' day-to-day practices.

Mr. Neffgen told reporters, "Our aim was to provide a good decision-making process for good judgment. We want people identifying, planning, and communicating key risks as early as possible. The framework creates this ability. When we view risk, we look not only at the negative aspects that can happen but also the opportunities to leverage risk to our benefit."

Analysis of American Express Lack of Risk Awareness

American Express (AMEX) took a very large risk that came back to haunt them. In one year alone, AMEX lost more than one billion pretax dollars, and, yet, the top executives were initially clueless about how it happened.

In 1997, AMEX began investing in risky high-yield junk bonds and other similar securities far more heavily than their competitors and higher than industry norms. As investments began to turn sour, both the CEO and the CFO did not have a handle on the problem (risk) nor the amount of the losses. The company failed to have a risk management officer whose responsibility is to review the portfolio of risk for what the company was investing in.

Some of the junk bonds they invested in were issued by struggling movie theater chains and companies hobbled by asbestos liabilities. But the problem did not start there. AMEX managers were under severe pressure to increase earnings. Despite having a successful advisory business, which consisted of 11,500 investment counselors who doled information and advice out to 2.5 million clients, AMEX had pretty much exhausted the profits they could make from this business. The advisory business was not growing fast enough to generate the top-down mandated profits. AMEX needed more than the incremental income earnings generated from selling investment advice.

An executive decision was made to juice up the company's investment mix as a result of the tremendous pressure being applied by the chairman, Harvey Golub. He demanded that the company achieve higher earnings growth or "heads would roll!" Employees within the company say the (former) chairman demanded that the Minneapolis-based unit of AMEX meet a return on equity growth of 20 percent, a highly aggressive amount for the industry.

The investment arm of AMEX decided to raise its junk bond portfolio to 12 percent of the $32 billion investment pool from a prior high of 8 percent. That strategy included investing more money in junk bonds than most of its blue chip competitors did. Thankfully, this risky strategy did not affect the $262 billion in assets that the company managed for its clients.

About the same time, another executive, who headed the high-yield investments, recommended that the firm go one step beyond junk bond investments and invest in the growing market for sophisticated financial instruments called Collateralized Debt Obligations or CDOs. Collateralized debt is supposed to spread the risk by tying together a large number of securities. At the time, CDO issuers were buying up the low-grade bonds of cable, telecommunications, and healthcare companies among others. They would package this shaky debt into new securities for sale. Even though the underlying bonds carried junk ratings, each new CDO was supposed to offer investors a portfolio with a broad range of risk. The riskiest aspect of the CDOs, which offered interest rates of 20 percent or greater, was that they were dubbed toxic waste by people in the market and were so risky that they did not as such merit a rating.

These high interest rates attracted AMEX's attention. With huge sums of money in its coffers from the insurance and annuities premium paid by its customers, AMEX dived into the CDO marketplace. Not only did the company buy securities from others, they also began packaging their own CDOs for sale through other investment houses. By being the issuer, AMEX doubled up on its exposure.

According to one insider quoted in a *Wall Street Journal* exposé, "We all went into it with our eyes wide open," and "We knew it was not going to be risk-free." However, within three years, all junk bond prices tumbled, causing some CDOs to be hit with downgrades at the same time that AMEX's junk bond portfolio was bombarded with defaults.

In the end, AMEX's entire high-yield investment portfolio deteriorated rapidly, and, because there were many different parts of the organization that were acting independently of one another, no one central employee or executive saw the disastrous big picture. Executives had been relying largely on reports generated by an outside CDO manager to evaluate the health and performance of AMEX's investment portfolio. It was not until a few senior executives sat down with AMEX's entire portfolio along with an in-house analyst that they saw the full picture regarding its entire portfolio exposure.

AMEX was able to recover from this fiasco. The lesson here is that this normally conservative business was under extreme pressure by the chairman to increase earnings. Empowered employees were able to enter aggressively into a high-risk exposure without the corresponding controls, checks and balances, or reporting mechanism to ensure that risk was carefully managed. The cost that AMEX could not afford was the loss of some key personnel, the public embarrassment, the billion dollar loss, and the 33 percent hit on its firm value.

Risk Awareness Tool

The Institute of Internal Auditors (IIA) is a great resource for information and tools to deal with the downsides of risk. Although their primary mission is to support the internal audit community, internal auditors are becoming a valuable member of the risk management team. For large companies, the internal auditor regularly examines operational areas where risks are likely to occur.

One of IIA's tools is this questionnaire aimed at leaders, executives, and board members to create awareness for them regarding risk. As you go through the questionnaire, see how many of these you can answer "yes" to. Each "no" answer is something you need to be more concerned about.

- Is there a process or function within the organization responsible for assessing and monitoring risk?
- Do I have assurance that controls are operating as planned?
- Is there a thorough and appropriate reporting mechanism within the organization that allows for adequate checks and balances for fraud prevention and risk management?
- Do I have assurance that financial and other information is reported correctly?
- Are risk management, control, and governance processes being evaluated and reviewed for efficiency and effectiveness on an ongoing basis?
- Do I have a clear understanding of enterprise-wide risk and the organization's key areas of vulnerability?
- Does the organization have an operational system for managing risk?
- Is there an internal process within the organization for adding value to and improving operations?
- Are the organization's stakeholders provided with reliable assurances that their investment is protected?
- If I were not a part of management or the board, would I be comfortable with the assurances provided to me as a stakeholder?
- Am I able to sleep at night without worrying about risk in the organization?
- Am I comfortable that all risks have been appropriately addressed?

Source: *The Institute of Internal Auditors* and the *Journal of Accountancy*, January 2000.

Summary: Importance of Step 1

Step 1 of an effective risk management program is necessary to ensure that every decision maker in your organization is on the same page about "coloring outside the lines." As you will discover in the next step, there are many different views of what is risky and what is not. Without a common or mutually accepted view of risk, employees have a blank check on "coloring outside the lines."

Because accountability is very important to successfully running an organization and ensuring that internal controls prevent unwarranted or illegal behaviors, your carefully crafted and thoughtful definition allows executives to create a standard and expectation. This accountability helps to ensure that your firm maintains the delicate balance between being innovative and rash risk taking. This is not an easy step to take but it strengthens your organization's ability to deal with whatever unforeseen risk Murphy throws at you.

6

Step Two—Examine Attitudes Toward Risks

After completing this chapter, you should

- be able to implement step 2 of your risk management plan.
- understand your own attitude toward risk taking.
- understand the uncertainty domino.
- see how the risk taking entrepreneur views risk.
- understand the motivation for someone who avoids taking risk.

Exercise: Determine Your Risk Tolerance

Exercise No. 1

Please answer these questions:

Do you take risks? Yes ___ No ___

How do you know that you do or do not take risks?

Is it because other people tell you that you do or do not?

Is your answer because of your definition of risk?

Exercise No. 2

Take this quick self-test by answering "yes" or "no." These five simple questions will give you an assessment of your risk inventory.

Yes	No	Question
		Do you sometimes have endless debates with yourself when you have to make an important decision—sometimes making no decision at all?
		Do you accept poor service from a waiter or clerk rather than speak up?
		Do you have a hard time making an emotional commitment to others?
		Do you find excuses to stop yourself from getting a better job, learning new skills, or taking advantage of similar opportunities for self-improvement?
		Do you let the disapproval of others keep you from doing things you want to do?

Any "yes" responses indicates that you probably shirk from taking significant risks. I know that some people may not like hearing that. However, in reality, there are many differing attitudes toward risks. Some people would do things that other people would not.

Exercise No. 3

Which of these activities would you define as risky?

____ Rock climbing

____ Racecar driving (on a racetrack) at more than 200 miles an hour

____ Flying commercially once a week

____ Flying your own plane

____ Sky diving solo

____ Driving a busy freeway at rush hour

____ Having children

Not every one of those will be seen by someone as a risky activity. For most of us, having a child or two is not risky, but what about five or ten children? Have I reached your "too much cost" threshold yet? We all know people who do not get married because the thought of having even one child is just too risky. Speaking of cost, have you priced a university education recently?

Yet, I will bet that you commute to and from work on a freeway. Insurance actuaries consider this to be a greater risk than your driving on a race track at 200 miles an hour. Which of these two activities do you consider more risky? There are race tracks where you can drive at high speeds for a fee. They have customers in the thousands.

The Second Step

Risk is all about how you view something.

I hope you're now convinced that people have differing attitudes toward risk taking. The basis for taking step 2 in your risk management program is to understand and acknowledge this. This impact is felt at the organizational level.

Let us examine risk management principles 1 and 2:

- People do not take risks because of fear.
- Risk taking is a necessity for individual and business success in this changing world.

Now we will return to the individual or "100-yard" view of risk.

Personal Risks

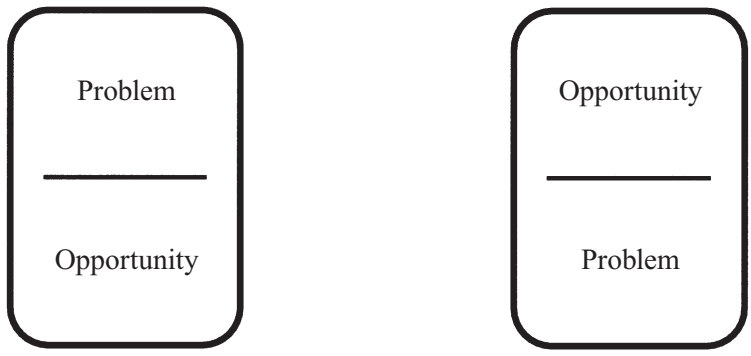
There are three major personal risks that we all fear and face:

1. Self-improvement risk:
   You wish to enrich your life for the better, yet self-improvement holds the possibility of FAILURE!
2. Commitment risk:
   You define yourself by the commitments you make, yet commitment holds the possibility of a WRONG CHOICE!
3. Self-disclosure risk:
   You must be honest with yourself (in other words, your feelings, your concerns, and so on) before you can disclose yourself to others, yet self-disclosure holds the possibility of REJECTION and HUMILIATION.

The Uncertainty Domino

When it comes to understanding how we look at risk, the uncertainty domino helps. I am not sure if you have ever played dominoes, but it is a fun game. Every domino tile contains two numbers. You can play the number on one side of the domino, or you can play the other number, so you always have two options. Similarly, how people look at risk can either be seen (like the domino) in two ways: as a problem or as an opportunity.

Exhibit 6-1
The Uncertainty Domino



Most of us in accounting and finance see risk as a problem. We understand what cost is, we know the dire implications of risk failure, and our own fears come into play. We see a risk as a problem because that little voice in our brain says, "I don't think we should be doing this!"

There are just as many in the world who see things like rock climbing or skydiving as great opportunities. They would define the choice as "a chance to try something new" or as "a thrilling experience."

This leads us to risk management principle 3:

- Risk taking is in the eye of the beholder.

Motivation Behind Avoiding Risk

Why do we take so few risks, especially with our money?

The fear of loss is the motivator for seeking gains. We (especially Americans) find losing money so distasteful that it blinds us to seeing risk as an opportunity to gain something. However, the elation that comes with winning is short-term compared to the feelings of shame and regret we hold onto whenever we lose. Our feelings of loss are much stronger than our drive for a gain. Similarly, failure in our past can sabotage our willingness or confidence to take a risk. This affects our optimism or belief that we can succeed again. This adopted attitude, at its worst, is that we will take no risk at all. Risk averse people tend to magnify the consequences of failure to the point that we lose sight of the upside. We must not let that happen if we choose to succeed!

While this has been a discussion of the individual view of risk, it also applies to an organization, because every team, company, and agency is made up of people. How we act as an individual is how we act as a group. Our fear of loss must not become an acceptable excuse to making progress or being innovative for the individual and for the organization. Individual egos make up the corporate ego.

Lesson of Step 2

The main lesson from implementing step 2 is simply this: people have differing views of what is risky and what is not. In step 1, your leaders defined for the whole company what is considered risky and what makes it risky. In other words they faced up to "What is the cost that you as the company cannot afford?" On a leadership team of 13 people, you will have 13 different opinions of what is a risky venture, because people always carry their own personal view of risk into the business setting. For every 100 employees, you will have 100 different definitions of the payoff or reward for taking a risk.

Your Firm's Specific Definition of Risk

In your firm, like all others, the correct answer to the question about what is a risky activity can vary. For example, if you are a startup company in your first years of existence and your funding is shaky, your definition of acceptable risk is going to be very limited. The opposite could also be true. Because you have little to lose, it may be acceptable to throw caution to the wind. Many successful firms started out this way, such as Apple and Microsoft.

If your company is well established and has survived at least 15 years, the definition of risk will be much broader and wider. Your leaders may decide that growing by 150 percent in one year is too risky, but growing incrementally at 30 percent per year is an acceptable risk.

What if your company is a multibillion dollar international conglomerate? Your leaders' definition of risk is going to be extremely different than the startup's definition.

From 1999 to 2004 we were in the middle of economic downturn. Interestingly, in this recession, the majority of our companies hunkered down, cut expenses, and strove to weather the storm. Yet a large number of organizations used that difficult period as an opportunity to go on merger or acquisition sprees, to spend more on research and development, to invest in new products or new customers, to create new channels, or to purchase new customers.

In 2008, we are undergoing another major downturn.
Does your firm have a strategy to:

a) Hunker down and take little risk, or

b) Take a risk such as growth, acquisition, or investment in the future?

Outsourcing as a Risk

Other farsighted organizations used the recession as an opportunity to streamline their operations and decide which functions to outsource. I have noticed that almost every issue of *BusinessWeek Magazine* over the last two years has contained an article about the cataclysmic change outsourcing is having on the business world.

Answer these questions:

Do you see outsourcing parts of your business operations as a risk or as an opportunity?

Why do you see outsourcing this way?

Do the executives of your firm see outsourcing as something you should or should not do?

Have they ever considered outsourcing?

Exercise: Taking a Risk

Think of a major risk you have taken in your life, either personal or business-related.

Tell a friend or colleague about this risk. Explain what you learned from this experience and, all things being equal, whether you would do it again.

Write down the major risk _____

_____

_____

_____

_____

Would you consider yourself to be a risk taker? Does your friend or colleague consider you to be a risk taker?

Which of the major personal risks did this activity explore (from the "Personal Risks" lists)?

What made this a risky activity?
How does this relate to the topic of managing risks?

The point of this activity is to show that while you may not define yourself as a risk taker, the person listening to your risk may look at it as something risky. Likewise, you might describe what you did as taking a risk, but the person you describe it to may not see it as a big risk taking adventure. It all boils down to how each individual person views risk and in finding the value or danger of any particular venture into the unknown.

The Mindset of the Risk Taking Entrepreneur

Call it a genetic compulsion, a defensive reaction, or simple optimism, but the reality is most business owners refuse to contemplate the possibility of failure. It is as if the word does not exist in their vocabulary. But failure is an option! The downside of this "never say die" attitude is that it can be ruinous, wasteful, costly, hurt people, and spoil opportunities for future success.

Most entrepreneurs see themselves as the type of person who put their heads down and charge full steam ahead. However you can badly injure yourself with that mindset. This person does not avoid risk, but ignores it at every opportunity. This person fails to recognize that failure is an option. This is why risk can be mismanaged or unacknowledged.

In facing up to the possibility of failure in risk taking, there is a very delicate line to walk. It is better to assume failure can occur than to resign yourself to it. It is okay to acknowledge our fear but not let ourselves to be overcome by it. Walking that line requires courage.

The Mindset of the Risk Averse Person

Even though (here in the United States) we prize and value people who take risks, there is a group of people who tend to be risk averse. We often describe this group as those *stuck in the mud accountants*.

Often, we say that we should take more risk because we see how risk taking is revered in our culture. Just look at the honors bestowed on Olympic athletes and poker players among others. However, when reality sets in, and we realize that we could actually lose money, others will see the type of risk takers we really are. Generally, people *hate* to lose money! *People hate to look stupid or incompetent!*

Back to Us

Folks in finance and accounting own the mentality, "I am the guardian of the assets," and this attitude leads us to look at risk differently.

When making a critical decision, taking risk is composed of the following:

- How emotional vs. how rational I am
- How confident vs. how anxious I am
- How impulsive vs. how reflective I am

Risk is inherent in nearly everything that a business does, including expansion, mergers, research, or contraction. Therefore, no matter how much you or I research a decision, we (as typical accountants) must face that there will always be uncertainty in any strategy and decision.

As a controller or CFO, I want to make sure that I do not do anything stupid. But that is very different from taking a risk. The Controller or CFO's job is to put forth the best alternative, suggest the pros and cons, identify the opportunities that we seek, and then show what the future could look like in both scenarios. While doing this evaluation of a risky situation, we must keep an eye on potential gains or upsides as well as the potential losses or costs.

Case Study

Analysis of Royal Bank of Canada Revisited Risk Definition

Royal Bank of Canada recently found that privacy was its key risk and turned that knowledge into an opportunity. The bank's privacy policy is centered on retaining and growing customers' trust and has become an integral part of the bank's overall strategy and everyday business practices. This meant that the bank needed to move to a higher level of privacy beyond meeting the minimum regulatory requirements.

Based upon customer feedback through research, the bank discovered that 83 percent of their customers would stop banking with them if they felt their information was being used inappropriately or was not being protected. Leaders recognized the tightrope they walked—protect the customer's information or use that information to provide better service. They recognized the need for acceptable balance. Therefore Royal Bank of Canada altered its strategy toward risk taking to the following: "Everything we do, every process we develop, has the customer balance at its root."

A 10½ Step Plan to Build Your Self-Confidence for Risking

1. Understand your tolerance level for risk
2. Recall that you have risked successfully many times before
3. Deal first with your anxiety for risk taking
4. Emphasize the reward or risk instead of the risk or reward ratio
5. Make decisions with less data to build your intuition
6. Do not overplay the significance or downside of the risk by asking: "What is really my cost?"
7. Rely on your intuition—it is usually right
8. Get the counsel of a risk taker you admire
9. Know that the cultural norms always affect individual risk taking
10. Know that you always have choices, no matter the initial outcome

10½. Remember that not all risking is risk taking

Answer this question:

What are these rules telling you about encouraging people to see risk differently?

10½ Rules of Creative Risk Taking

1. All risk taking involves a choice.
2. All risk taking requires an investment.
3. All risk taking can fail.
4. Risk takers put themselves and their ego on the line.
5. All risk taking is accompanied by feelings of stretching or rising to the challenge.
6. All risk taking requires facing our anxieties:

    a. Humiliation
    b. Failure
    c. Wrong Choice
    d. Rejection

7. All risk taking carries important psychological rewards.
8. Virtually all risk taking sparks feelings of excitement, novelty, movement, and change.
9. Every risk taker remembers experiences of prior risks taken.
10. Risk taking is *not* gambling.

10½. Take risks—or die!

Answer this question:

What are these rules telling you about risk management in a business?

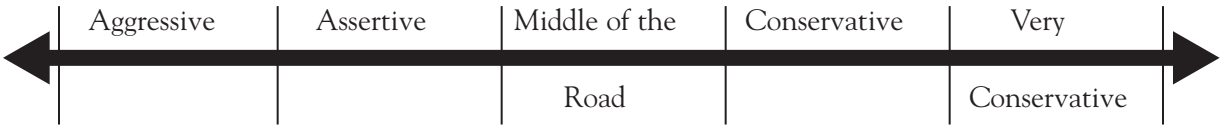
Exercise: Who Is Running the Train?

Instructions

In the table below, think of five areas where your firm regularly faces or takes risks. List them. Next enter the name of the person who is responsible for managing the area at risk. Last, think about that person's individual approach to risk taking.

Spectrum of Attitudes Toward Risk Taking:

Flying Without a Net **Black and White**



Risk Area	Person Managing this Risk	Person's Attitude Toward Risk Taking
Example:		
Sarbanes-Oxley compliance	Treasurer	Very conservative
1.		
2.		
3.		
4.		
5.		

Answer these questions:

What did you notice about the prevailing attitudes toward risk taking in the people that are "running the train" in your firm?

Is the attitude of the person managing your risk area appropriate, too much, or inadequate?

Is there a balanced view in your organization?

Summary: Importance of Step 2

If your firm fails to take step 2, and immediately proceeds to step 3, *your risk management program may fail*. Your management team, like all others, is made up of different individual mindsets toward risk taking and the cost of failure. If these individual mindsets are not addressed openly, every action plan and every strategy will not have the value of balance. This delicate teeter-totter between being innovative and protecting ourselves is critical to having an effective risk management plan.

We must not let the "cost-conscious, bean-counter" mentality slow down our need to innovate. We cannot let the "there is unlimited possibility" mentality foster unwarranted risk and reckless decision making. Step 2 emphasizes the need for both views of risk as a catalyst for achieving ever greater success.

"If you refuse to take chances, you are stuck, which today is taking a step backwards!"
—Ron Rael

7

Step Three—Analyze the Firm's Ability to Handle Risk

After completing this chapter, you should be able to

- describe to others the impact that corporate culture has on risk management.
- look for specific risks in an organization's key strategies.
- describe, from a self-assessment, the level of accountability that people display in your organization.
- describe for others how the three budgets, the operating plan, and the financing plan are used in managing risk.
- ply the risk-by-identification tool to analyze a specific risk.
- use the ideas in this chapter to foster a culture that balances risk taking with risk exposure.

Case Study

Analysis of Amazon's Ability to Take Risks

Another example of an ultimate risk taker is Jeff Bezos, the founder and CEO of Amazon.com. Jeff is confident that his organization can take big risks and survive. For example, Amazon ventured into the furniture business, even though that proved to be unfeasible at first. Today, Amazon uses its Web site as a pull-through for vendors such as Art.com and The Bombay Company Inc. Then, Jeff's company started the Z stores, and now that risk brings tremendous revenues without much cost. Jeff and his team continue to foster relationships with other organizations, such as Toys "R" Us and Martha Stewart Living. Some of these partnerships have succeeded and some have flamed out, but Amazon continues to take big risks within the framework of its business model.

Back in 1997, so-called experts predicted that with the launch of BarnesandNoble.com, Amazon was going to soon be "Amazon.toast," but Amazon thrived and expanded. As 2000 approached, Amazon's share price fell from $100 to $6, but Jeff Bezos did not see this as failure. Amazon posted its first real profits in 2003 and is on track to exceed $11 billion in sales, growing at an annualized 16 percent. Meanwhile, as of February 2006, the stock was at $39 a share, giving it a market value of nearly $17 billion. Amazon is among EBay, Yahoo, and a few others who endured as the survivors of the Internet Age, using the lessons learned from the "dotbombs" to build successful organizations with viable business models.

Currently, July 2008, Wall Street is bullish on Amazon and its stock price has hovered in the $70 to $80 range.

Fast Company Magazine's August 2004 issue featured a Jeff Bezos interview by Alan Deutschman ("In the Mind of Jeff Bezos") about some of the changes that Amazon is contemplating. According to Deutschman,

Jeff Bezos is "the ultimate quant jock" because he relies heavily on intuition and insight. He is described as having boundless enthusiasm combined with outrageously good luck.

Jeff Bezos credits his legendary luck to creative innovation. Jeff uses farsighted thinking and relies on his intuition. Yet he is also a "by the numbers" boss who prefers to measure everything using spreadsheets. He bases most of his critical decisions on this data, not judgment or instinct. Jeff uses numbered lists for all things that he needs to do. What separates Jeff Bezos from his less successful colleagues are his nightmarish (to some) leaps of faith. His best decisions cannot be backed up by studies or spreadsheets. He makes nervy gambles on ideas that to outsiders seem too big or too audacious and not bottom-line oriented. Jeff introduced innovations that initially hurt Amazon's sales and profits for the short run, yet turned out to be the right decisions. They increased customers, which in turn increased profits. The culture that Jeff has created is adept at coming up with innovations. Yet he employs best practices to learn from other successful businesses and from competitors.

Jeff Bezos is described as the rare leader who gets excited over finding small improvements and efficiencies within Amazon's operations, while maintaining a grand vision of a changing world. He is both stubborn and flexible at the same time.

Another example of Jeff's thinking is to go against the prevailing generally accepted notion that good communication is important. Jeff believes "communication is terrible." He adopted within Amazon the concept of the "two-pizza team," which means that if you cannot feed a team on two pizzas, then the team has too many members. It is within Amazon's two-pizza teams that their innovation is fostered. These teams create some of the quirkiest and most popular features on the Amazon site. Jeff is constantly testing the marketplace and taking large risks to see if his intuition pays off. Sometimes it works and sometimes it does not. An example is the *Bottom of the Page Specials*. These are items you would not find at the traditional bricks and mortar bookstore: toilet paper, watches, and blenders. Of course, you can find bargain books there too.

To sum it up, by relying on the numbers, his team's best instincts and judgments, and his instincts, Jeff Bezos practices effective risk management. He is willing to take large risks while understanding their cost. At the same time, he knows that his risks can be wasteful, and he makes sure that he has confidence both in the numbers and his people.

Case Studies to Learn From

To help you understand how step 3 works, we will explore two risk taking companies, Costco and Men's Wearhouse. You will have information on both companies, highlighting the specific strategies each one uses to stay successful.

Exercise: Risk Analysis

Instructions

Select one of the two companies. Your goal is to select a specific strategy of that organization and write down as many risk exposures to the strategy that you see. Assume that you are an investor or on the board of directors of your selected company, and you are presented this new strategy. It is your responsibility to critique it. You can be hypercritical. Look at the strategy and list all your concerns. Be sure that you can justify your concerns to someone so that you refrain from basing your analysis on your personal fears.

Case No. 1—How Risky Is Costco's Strategy?

Read the summary of Costco's strategy starting on the following page. Select one or two strategies Costco employs to retain its advantage. List the potential risks Costco faces with each strategy in the following chart.

Costco's Strategy Element	Costco's Risk Exposure(s)

Costco's Strategy for Competitive Advantage

Costco's Business Strategies. Goal: To reinforce its reputation for quality products at low prices and enhance membership value by

1. creating merchandise excitement.
2. providing ancillary services.
3. growing private label offerings.
4. introducing more business membership opportunities.
5. maintaining well-run facilities and operating efficiencies.
6. monitoring price savings on all items and leverage over suppliers.

Costco's strategy is based on the concept of offering members very low prices on a limited selection of nationally branded and selected private label products in a wide range of merchandise categories. This produces rapid inventory turnover and high sales volumes. When combined with the operating efficiencies achieved by volume purchasing, efficient distribution, and reduced handling of merchandise in no-frills, self-service warehouse facilities, Costco is able to operate profitably at significantly lower gross margins than traditional wholesalers, discount retailers, and supermarkets.

Costco's mission statement and firm commitment is: "To continually provide our members with quality goods and services at the lowest possible prices." The emphasis is on combining both high quality merchandise and low prices, not on offering the cheapest prices.

Costco is somewhat unique in its approach to the market. Of the three sustainable competitive advantages—cost leadership, differentiation of product, or focus on a market niche—it could be argued that Costco is working to achieve all three. Costco is not the place to go to buy the lowest price item in a product category, but if the customer is looking for the lowest price on a high quality product, then Costco can deliver what the customer wants. This is the area in which Costco has cost leadership.

In the area of product differentiation, Costco provides a range of high quality, name brand products (at low prices), and, in some product categories, they also offer their own private-label offerings at attractively low prices. These private-label products are the same high quality as national name brands, but Costco can sell these items at a lower price because they do not have the expense of advertising, which is a component of the price of name brand products.

Some might also argue that Costco has found a market niche. Because their business is based on a membership concept (whereby members pay an annual membership fee in return for the opportunity to purchase quality products at low prices), Costco appeals to consumers that can afford the membership fee and are knowledgeable about the variety of products, levels of quality, and prices available in the marketplace. These customers have a higher-than-average family income and have demonstrated strong customer loyalty to Costco by renewing their memberships at a rate of approximately 97 percent.

Case No. 2—How Risky Is The Men's Wearhouse Strategy?

Read the summary of The Men's Wearhouse strategy on the following page. Select one or two strategies The Men's Wearhouse employs to retain its advantage. List the potential risks TMW faces with each strategy in the chart that follows.

The Men's Wearhouse Strategy Element	The Men's Wearhouse Risk Exposure(s)

The Men's Wearhouse: Success in a Declining Industry

The Men's Wearhouse Global Business Strategy.

1. The company positions itself as a high quality, yet lower price, store of choice for business clothing.
2. They target the up-and-coming professional who has a need for a sharp and polished look as an alternative to the more expensive Nordstrom and Brooks Brother's labels.
3. The selection of clothing is limited and changes several times a year to keep up with current trends.
4. They sell the lesser quality products of well-known brands.
5. The stores are located in the shadow of their direct competition.
6. The rental of men's wedding wear is a major profit center.

"We're in the people business, not the suit business." George Zimmer, chairman, May 1997.

"Our distinguishing feature is how we treat our employees. You cannot tell them to treat your customers like kings and not treat employees like kings." Richard Goldman, executive vice president, August 1996.

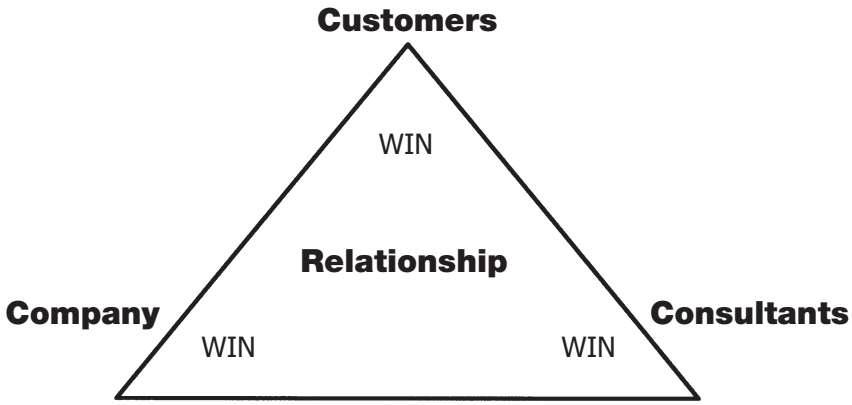
"Our mission at The Men's Wearhouse is to maximize sales, provide value to our customers, and give quality customer service, while having fun and maintaining our values. These values include nurturing creativity, growing together, admitting to our mistakes, promoting a happy, healthy lifestyle, enhancing a sense of community and striving to become self-actualized people."

Company Goals. The Men's Wearhouse sets these measurable targets:

- Increase volume
- Minimize shrinkage
- Provide outstanding customer service
- Provide a high-quality work environment

The company seeks to hit these targets by nurturing a Win-Win-Win relationship, as shown in exhibit 7-1. The Men's Wearhouse designates their people as consultants, not employees.

Exhibit 7-1
The Men's Wearhouse Mission



Source: *Stanford University Graduate School of Business case study HR-5*

The Point

The lesson in this activity is that a critical piece of any reality-based planning process is to examine the risks associated with each strategy in your business plan. The source of risk in every business organization comes from one place, which will be explained further, later in the chapter, and the person who promulgates that risk is usually the founder, CEO, president, or the significant decision maker.

Risk of Weak Accountability

Take this single self-test on accountability and be as honest as possible.

After you have completed for yourself and your organization, read the answer key below to understand the risk that currently exists within your organization.

Exercise: Accountability Self-Assessment

Instructions

Rate your company (or department) on each item to determine how well your firm or team displays accountability. Be brutally honest!

This is how my boss acts:

He rarely does what he or she says he or she will do.			He or she usually follows through.		His or her words and actions always agree.	
1	2	3	4	5	6	7

This is how we follow through on our commitments to one another:

We ignore one another's needs.			We try to support one another		Every person feels supported.	
1	2	3	4	5	6	7

This is how we follow through on our commitments to outsiders:

We laugh when they ask for help.			We often deliver what we promise.		Outsiders are always pleased.	
1	2	3	4	5	6	7

This is how we hold each other responsible when someone does not follow through:

The person gets away with it.			Sometimes the person is talked to.		Follow-up is immediate.	
1	2	3	4	5	6	7

This is what happens when something goes wrong:

The focus is on who goofed.			We blame and then fix the problem.		We focus on how to prevent it again.	
1	2	3	4	5	6	7

Answer this question:

Because the 6 and 7 scores show maximum accountability, what does this tell you about the level of accountability existing within your company?

Answer Key

If you rated your organization or your boss as "1" or "2" then you are not being honest or *you need to work for a new company*. If you rated your organization or your boss as "6" or "7," then you are also not being honest because you have a narrow view of the situation.

More realistically, in each of the five scenarios you would have rated your firm or team between 3 and 5.

Why? Because accountability is an attitude and a choice, and just like every choice, some days we feel like making the choice, and some days we do not. It is impossible for anyone to be accountable every moment of the day. Things occur and events happen where we suddenly and immediately play the blame card or we make a commitment, and then we forget about it or fail to follow through. Real life happens. What I want you to examine in the self-assessment is the overall attitude within your organization that people have toward accountability.

The Point

The lesson in this activity is that accountability is the cornerstone for a balanced risk management plan. If people refuse to act in an accountable manner, they will shirk their responsibilities for reducing unnecessary or costly risk.

What happens if the executive or the board is asleep at the wheel and they are not concerned about risk? You have Kmart, Sears, WorldCom, or Merck; the list grows every day.

Therefore, as financial executives, we must understand that the major source of your firm's risk is the impact that leaders play in coming up with and implementing a strategy. This is why including a proper risk management program is a must!

Now let us turn to this source of almost all business risk: your strategic plan.

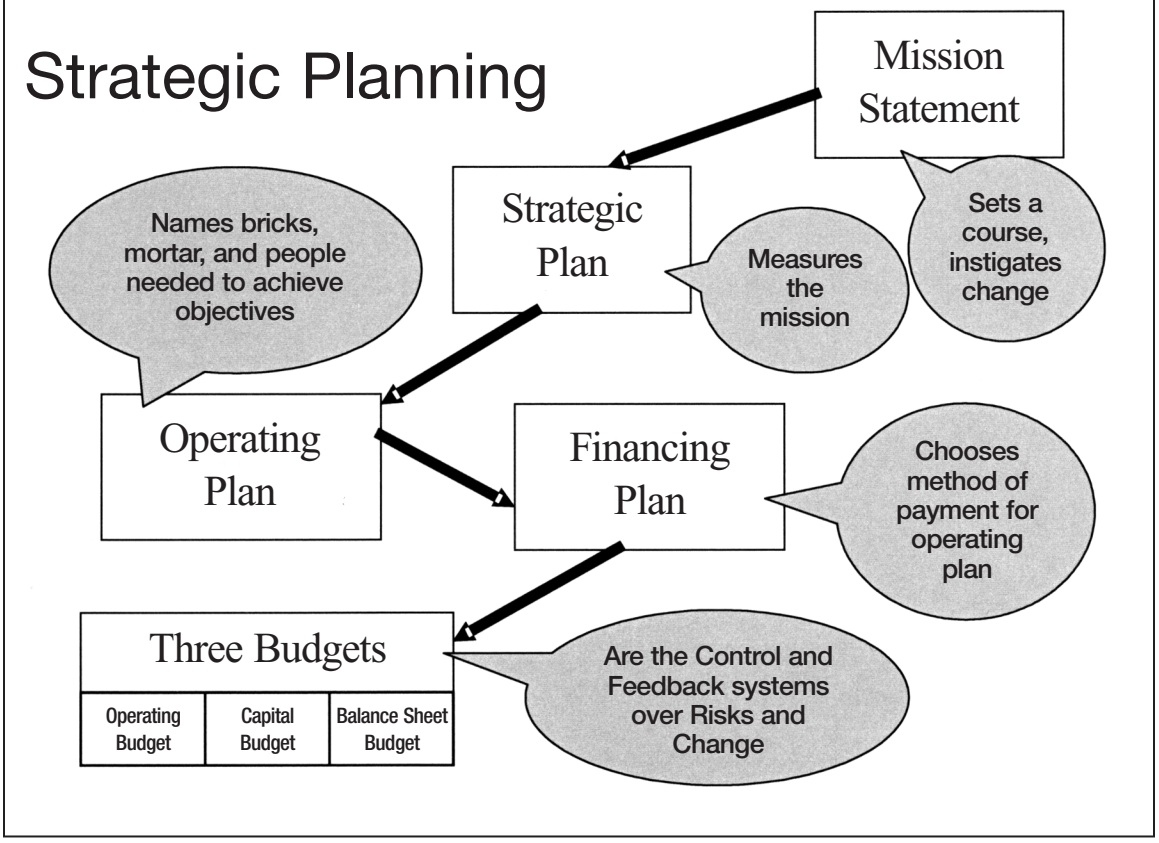
Answer this question:

What is strategic planning?

The Source of All Business Risks

Strategic planning is managing change and overcoming risks. Strategic planning is a process where risk can be identified and dealt with.

Exhibit 7-2
Strategic Planning Flowchart



Strategic planning starts with your mission statement because it sets the organization on a course and instigates change—from today's status quo to where we want to be in the future.

The second element of strategic planning is your actual strategic plan, the measurement of your mission. In this document you identify specific metrics and methods of measuring whether or not you are accomplishing your mission over the next 18-24 months.

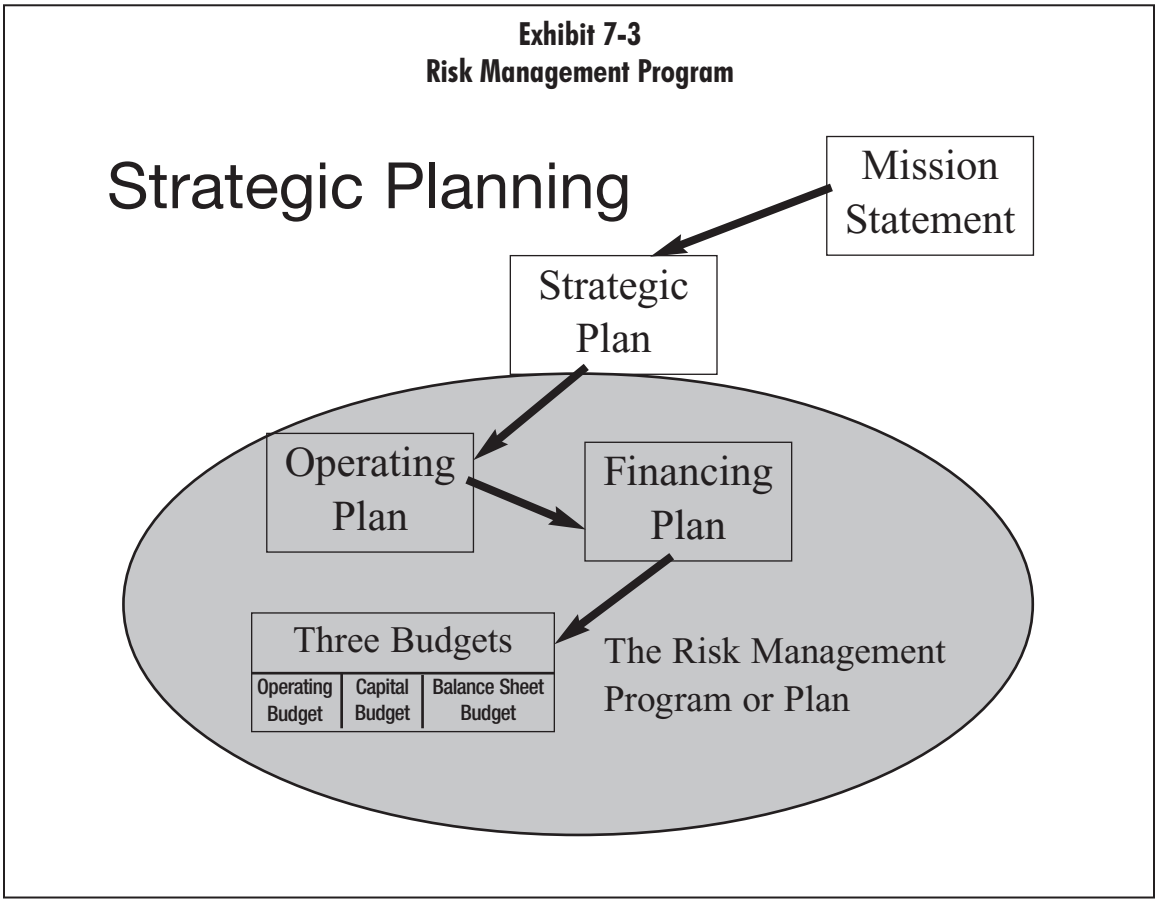
Information from the strategic plan flows into the operating plan, which identifies the bricks, mortar, and people you need to achieve each specific objective in your strategic plan. The operating plan is where we are headed and what we will commit to accomplishing in the next 12 months.

Out of your operating plan comes your financing plan. In this document you highlight the methods of payment for the bricks, mortar, and people in your operating plan. For instance, how much of the money will come from internal sources and profits? Will some of the funds come from outside investors? Will addi-

tional funding be required from our banks or other lenders? These are the questions that get answered in the financing plan.

Finally, from the financing plan, you develop your budgets: the operating budget, the capital budget, and the balance sheet budget. These three documents become your control and feedback systems over the risks and the changes that you started with your mission and strategy. This is a holistic look at your planning continuum that reminds us: "We really need to plan carefully."

Exhibit 7-3
Risk Management Program



Your global risk management program consists of your operating plan, financing plan, and the three budgets. *What goes terribly wrong in most organizations today is that the leaders see risk management as a function of insurance*. This job is assigned to the CFO or a risk manager, a position that today many firms have outsourced or eliminated. The risk manager is rarely included in the strategic planning process. What this means is that your executives embark on a global plan, ignoring the risk or underestimating the risks' cost, and then turn the risk analysis over to the CFO or risk manager. They drop it in the risk manager or CFO's lap and ask, "Do we have adequate insurance coverage for this particular risk?"

This is a fatal blunder!

As you can see from the "Strategic Planning Flowchart" (exhibit 7-2), this will not really protect the firm. The risk management program needs to be a key agenda item of strategic planning done offsite when the leaders figure out what the plans are for next year. This is also the time they define what is risk as described in step 1.

As you saw in chapter 3 on enterprise risk management (ERM), good risk management requires a team approach. An effective ERM program consists of a cross-functional team of people throughout the organization who examine risk holistically.

Risk's Two Faces

Now that we understand where risk starts (your strategic plan) and that risk management planning goes hand in glove with strategic planning, let us take a look at some planning paradoxes to understand how the organization can effectively face up to risk:

- Paradox No. 1 of Risk Taking
  - Mistakes are an inevitable part of learning.
  - Mistakes waste money and resources.
- Paradox No. 2 of Risk Taking
  - A business is not growing if it is not risking.
  - Business failures often result from the negative impact of risks taken.
- Paradox No. 3 of Risk Taking
  - The culture of the organization must be risk tolerant.
  - The culture must be able to expose areas sensitive to risks.
- Paradox No. 4 of Risk Taking
  - Taking risks is facing the unknown.
  - Leaders exist to reduce uncertainty.

Answer this question:

What are these four paradoxes saying to you?

Answers I hear most often are as follows:

- "They are saying damned if we do, damned if we don't."
- "They are saying risk is inevitable."
- "They tell me that as CFOs we must be concerned about both sides of risk."
- "These paradoxes basically say that risk is inevitable, but we can do things to plan for them."

In a nutshell, what these paradoxes, together, are saying is that we cannot know everything, so we must be able to handle whatever risk occurs, especially those that we cannot foresee.

Answer this question:

How do these four paradoxes particularly affect controllers and CFOs?

Accounting Sits in the Middle

We in accounting and finance, especially if you are a controller or CFO, are the people in the middle. We are in the midst of a very delicate high wire act, and we must make sure that we manage this balance very carefully. We cannot afford to push the organization too far on one side. If we focus solely on the controls and checks and balances or we are anal about people crossing all the t's and dotting the i's, we foster a culture where no one is willing to take any risk. History is littered with businesses that failed to out-innovate their competitors or keep up with the evolving marketplace.

On the other side of the balancing act, we have employees and leaders who want to be innovative, who strive to be creative, and who push the envelope on innovation, ideas, and processes. Our job is to support them *and* not let them undermine the success of the organization. Why? For every company that has gone out of business because it failed to be innovative, there is a company that is history because they did not manage the risks they took.

The Cultural Aspect of Risk Taking and Risk Management

Write out how you would define workplace culture.

To me, workplace culture is …

Your definition of culture is nearly the same as mine because culture is instinctual in us. Any time two or three people join to work together on something, they create a culture. It is something that we humans do naturally.

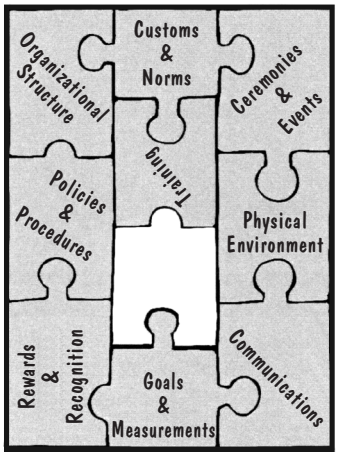
Workplace culture is the mood, attitude, and atmosphere of an organization. It is the story of who we are as enacted by each employee. A shorthand for describing culture is: "How things are done around here."

What you may not know about culture (even though you have a good intuitive sense of what it is) is that culture is made up of ten unique pieces. These ten pieces fit together like a mosaic, and each one affects the other. They all must be in place for the mosaic to exist and they must create a cohesive picture or image to be useful.

Exhibit 7-4
Culture Mosaic

The Cultural Mosaic Components:

- Communications
- Customs and Norms
- Physical Environment
- Rules and Policies
- Training
- Ceremonies and Events
- Goals and Measurement Process
- Leader's Attitudes, Behaviors, Beliefs
- Organizational Structure
- Rewards and Recognition



Your Culture Mosaic

Exhibit 7-4 is an image of how the mosaic pieces meld together. The centerpiece of all culture mosaics is the leader's attitudes, behaviors, and beliefs. This leader can be one person, a team, or a family.

When individuals decide to form an organization or start a business, they gather other people around them who have a like mind. We all have heard this description of some small businesses: "We are like a family." This describes a firm that consists of like-minded people sharing the same values and visions. All businesses start out this way, even Wal-Mart, IBM, and Ford Motor Company.

Then, as the organization grows and matures, the leader, realizing the need for additional help, installs channels of communication. The firm grows into different physical locations and each with its own environment. The leader has to set rules and policies to shape other people's behaviors. The organization sets goals and tools to measure those goals. Because we want to reward people and maybe share the profits, we establish awards and recognition programs. We create an organizational structure because people have to fill specific slots, wear fewer hats, or take on certain roles. Of course to promote fun, the leaders sponsor a Christmas party, Fourth of July picnic, or monthly potluck birthday celebrations. Sometimes on their own or with guidance, employees start forming customs and norms, like the end of the month beer bash and casual Fridays. But, notice the center of the culture is still the leader's attitudes, behaviors, and beliefs. This centerpiece drives the entire culture from the beginning.

As the company grows older and the leader decides to hire professional managers because current leaders cannot do everything themselves or perhaps have grown incompetent, new leaders come in and start putting their imprint on the culture with new attitudes, behaviors, and beliefs. Even if this occurs, it takes years for the attitude, behavior, and belief of the original founder to be fully removed.

For example, even though Bill Gates has not been Microsoft's CEO for nearly a decade, when he replaced himself with another culturalist, Steve Ballmer, there is still a lot of Bill Gates in the DNA or culture of Microsoft.

In Seattle, there is an organization known as Foss Maritime, which provides comprehensive marine transportation and logistics services. This company is well over 100 years old and is still owned and led by the Foss family. The DNA or corporate culture of Foss to this day contains the imprint of the original Foss founders.

By now you are thinking, "Well this is great, Mr. Expert, but I am not a culturalist like Jack Welch or Steve Ballmer. I am only a small cog in the wheel, so what can I do about our culture?" I am glad you asked that question because that is where we are going next.

Visible Clues about Risk in Your Culture Norms

There are some visible outcomes in your culture that will tell you what the organization is like and what the culture says about its ability to handle risk. The areas that you need to keep your eye on and, if you are an auditor, need to examine carefully, include the following:

- Morale
- Sense of urgency
- Level of integrity
- Internal reputation
- Employees' attitudes
- Trust
- Behaviors involving ethics
- Loyalty
- Level of fun
- Cooperation
- Turnover rates
- Openness to the truth

Answer this question:

Why would knowing how your culture is built help you analyze your firm's ability to handle business risks?

Answers I most often receive include the following:

- "I would know if I should be concerned."
- "I could determine who most likely would follow through, and who wouldn't."
- "I could change the reward system to reward more risk taking."
- "We could evaluate the risky goals and get better feedback to determine if we're on track or should worry."
- "I believe that if employees are behind us [leaders], then we will more likely be successful, but if employees are against us, then our risk becomes greater."

That leads us to three more truisms of risk taking.

Risk management principles 4–6:

- Assessing and monitoring your culture will give you information about where you are vulnerable.
- Assessing and monitoring your culture will give you information on how your organization values risk taking.
- Most organizations do not perform any formal risk analysis.

Morale Is Vital In Risk Awareness

You must always stay aware of employee morale and look to see if and when it changes. If it changes above or below the norm, you need to ask why. Maybe the morale has gone up temporarily because there is a surge in new sales orders. Or maybe morale has gone down and unbeknownst to you most of your employees are going to jump ship. Recently a consultant in the human resources field cited several surveys that found over 80 percent of employees are unhappy at work because they do not like their jobs or employer, and they are actively looking for something else. Similarly 82 percents of executives are currently looking for new jobs!

Yikes!

Assume you are the CFO of an organization undertaking a strategic initiative that generates a major risk. If you are successful, it will grow the company, but if not successful it will bankrupt the company. Would you (as CFO) want to know that 82 percent of your executive team are about to leave? Would that change your level of concern about the risk? Would you change how you look at the cost side of the risk?

Understanding your culture is important to proper risk management! Another reason why it is important is that you want to change employees' attitudes toward taking more or less risks.

Culture Must Never Be Downplayed

In essence, culture is important because your culture brings forth success and failure with equal efficiency.

Culture is important, because the culture needs to expose risks rather than hide them. I worked for several organizations where the norm was to hide risk, because the leaders always shot the messenger! Rather than hear bad news, the leaders wanted people to dwell on the good news. In addition, they never wanted anyone to question or critique the strategies they thought up. So the prevailing culture became one where employees would do anything to save their jobs, which included sweeping unnecessary risks and problems under the rug.

Case Study

Analysis of Starbucks Culture and Risk

An example of what happens when people do not pay attention to or understand the concept of risk taking comes from a personal experience. I did some consulting work with Starbucks back in 1996, well before Starbucks had grown to the size it is now.

Back then, Howard Schultz's mantra was "2000 by 2000" meaning, "We will have 2,000 locations by the year 2000." In the period I was engaged by Starbucks, they had about 1,200 locations. There were a lot of nonbelievers outside of Starbucks (and a few inside) who said that would be impossible. People kept asking the question: "Why would anybody be willing to pay $3 for coffee when they can pay $1 at a Denny's?"

Sure enough, not only did Starbucks exceed 2,000 locations by January 2000, they are currently at somewhere approaching 12,000 locations with the goal of reaching 32,000 by the year 2010. Because of their culture of innovative risk taking and an ERM program, Starbucks will probably exceed that goal as well. However, they have not always had a good risk management program.

One of the Starbucks employees on my project team told me an enlightening story. It was a tale of what happens if risks are not analyzed in advance. Before Starbucks came out with the Frappuccino as its own product line, they entered into a joint venture with another organization to create a Frappuccino ice cream to be sold through retail grocers. In this venture, Starbucks would provide the brand name and the partner would make it. They launched the product. Not too long after the launch, Starbucks accounting was asked to crunch the contract's numbers. Someone in accounting discovered that for every pint of ice cream sold under the Frappuccino name Starbucks lost $2.00. Starbucks locked themselves into a two year contract with this organization and could not modify the terms. Ouch!

This story reminds us that everybody who will be affected by a risk must be involved in the discussion about the cost or potential impact. Accounting is very often not invited to the table when risks are explored maybe because the leaders know that we have the ability to look beyond the hype or upside potential of the risk. Yet, this critiquing is crucial to a reliable risk management program.

Risk Analysis Tools

In a recent survey of CFOs and controllers, when asked if they use tools to quantify risk, they confessed that only one in ten use any tools like these. *What does that say about the future of those nine out of ten risk management programs?*

Tools of Risk Identification

This is a two-part tool using questions and a flow chart that will help you, as a leader, to look at risk differently.

Part one of the tool is six very important questions that need to be asked before a risk is undertaken.

Part two of this tool is known as the critical risk path. Walking through this, step-by-step, before the organization takes a major risk will help leaders and others to make smarter decisions.

Exhibit 7-5
Part One—Critical Risk Questions

What is the worst that can happen?

What is the best that can happen?

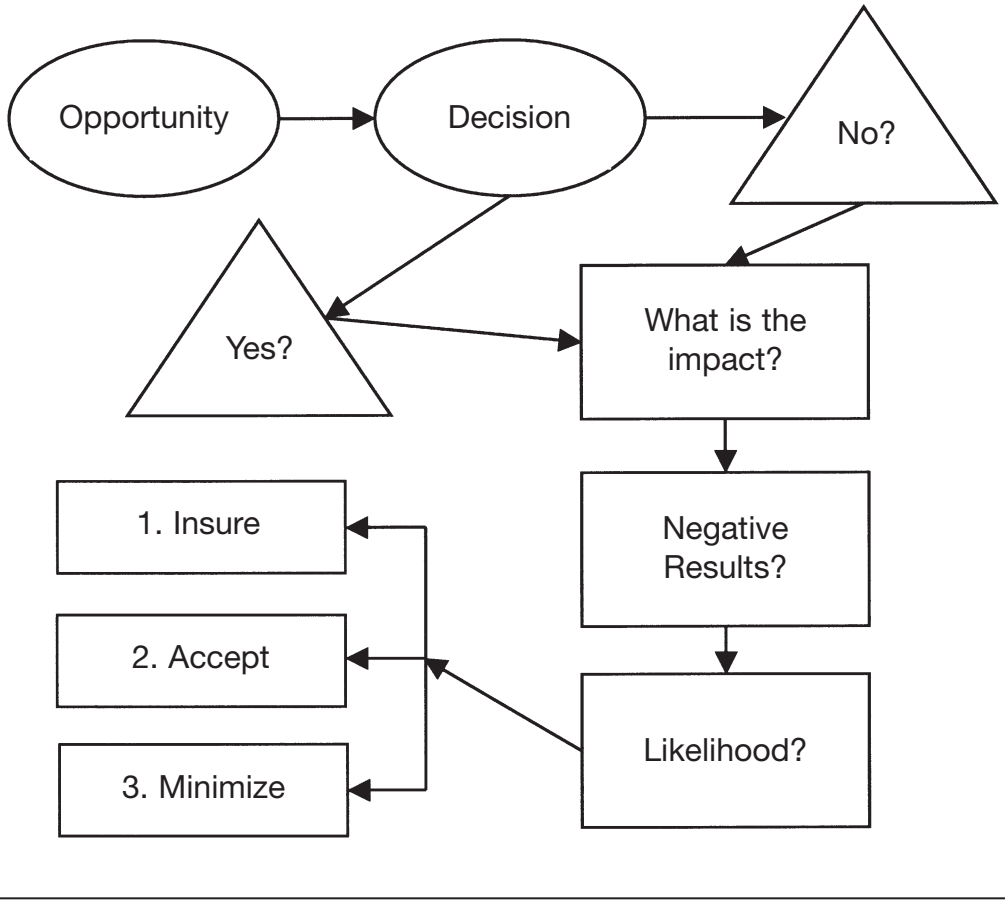
What is the most likely outcome?

What are the negative effects of the likely outcome?

How can we handle the negative effects?

How will we minimize or protect ourselves against the negative effects?

Exhibit 7-6
Part Two – Critical Risk Path



Let us see how they work together. Your firm sees an opportunity, for example, to do business in Russia. It is risky because you do not have any experience doing business there, and you hear stories about the crime and corruption that currently exist in Russia.

The upside of this opportunity is that there is a clear demand for your product with almost no competition. If you do not act swiftly, someone else could beat you there.

The question is: Do you open a sales branch in Russia, yes or no? Do not assume that this tool is simplistic, because its value lies in what comes after your initial decision.

So you say "yes," we are going to open a branch in Russia.

Let us go to:

- *What is the impact?*
- *How will your business model change?*
- *How will you get the product there?*
- *How will you handle returns?*
- *What commission structure will work there?*
- *Will this affect your current customer base and, if so, how?*

These are the sorts of concerns that will be addressed in question 2.

You have identified the impact, so then you go to the next question.

- *What are the negative results?*

This is a great time to commence the dialog on the potential pitfalls of the things that could hurt you.

- *How do we deal with the corruption issue should it happen?*
- *How do we protect our employees' safety?*
- *Because we are using contract sales reps, how can we ensure that our sales reps know the product?*
- *How do we prevent someone from pirating our design?*

The next question is very important because you now have to quantify the risk.

- *What is the likelihood of these negative results occurring?*

This is the heart of Sarbanes-Oxley, which requires leaders go through and quantify their risk. You do this by first listing each of the possible negative consequences and assigning a numerical likelihood. With experience, you will able to arrive at your own scale of probability. Then your leaders have not only complied with Sarbanes-Oxley, but they spent quality time analyzing each risk to determine the value of the risk.

Then, once you have a determined likelihood, you move to the choices you have to deal with the risk. One option is to accept it (knowing that the cost cannot hurt you). Another option is to minimize the risk. There are plenty of actions to take before undertaking the risk to keep its impact or cost low. A third option is to insure, but that does not mean that insurance is your only option. Sharing the risk, such as partnering with another firm or putting a stop-loss through a limited investment of both time and money, are ways to insure the risk.

Best of all, your three options are not mutually exclusive. For example, you could accept part of the risk, insure part of it, and closely manage it so that you minimize the potential downsides.

Tool for Breaking Down a Risk into Manageable Actions

This tool, which is known as a givens, negotiables, and controllables analysis, allows you to identify some of the specific actions you can take in order to minimize or mitigate the risk. To help you understand how the tool works, we will examine the risk of using purchasing cards. A number of companies are using purchasing cards, and every CFO or controller has warned others that you must go into this with your eyes wide open. It is not a simple solution, nor is it easy to implement. Most importantly, there are things that you must change or address within your organization and your culture in order to successfully use purchasing cards.

Steps

1. Write out a clear description of the risk to be undertaken:

   Soon we will begin using and issuing purchasing cards for every manager and supervisor. Most managers and supervisors are not trained adequately to deal with sales tax and account code issues. No extra resources will be available to handle the additional administration of purchasing cards.

2. Prepare a chart that describes the various aspects:

Givens **Aspects of the risk that we cannot control.**	**Negotiables** **Aspects of the risk that we can influence or minimize.**	**Controllables** **Aspects of the risk that we can use to address the danger.**
We must use purchasing cards for all supplies and related buys under $5,000.		
We do not know if our existing vendors will accept purchasing cards.		
We must be able to handle the administration of P cards within existing A/P structure and staffing.		
The purchasing employee, who supported A/P, is no longer a resource for us.		
The cards can contain only one G/L account number.		
All managers will be issued a P card for use by their department.		

In this example you will see that there are certain things that we have to accept, known as the *givens*. Second, there are parts of the risk that we can use to influence or minimize. These are known as the *negotiables*. Third, there are aspects of the risk that we can use to reduce the danger, and these are the *controllables*.

Exercise: What Would You Need?

In the space provided in the previous chart, list some of the actions, either negotiable or controllable in nature, that you would want in place to minimize the risk in using purchasing cards.

Exercise: Givens, Negotiables, and Controllables

Use the chart that follows to analyze your firm's recent innovation to breakdown a specific risk and define the givens. Then, decide upon both things that you would ask for or put into place to protect the firm. Do not be too concerned whether your suggestions fall into the negotiable or controllable column.

Write out a clear description of the risk to be undertaken:

Givens **Aspects of the risk that we cannot control.**	**Negotiables** **Aspects of the risk that we can influence or minimize.**	**Controllables** **Aspects of the risk that we can use to address the danger.**

Answer this question:

What did you discover or learn about being able to minimize risks using this particular tool?

In Essence

In step 3, you analyze the firm's ability to risk. It is very important for you as a leader and emerging risk manager to look at your culture. Let us end this section with a peek at what a culture that balances risk taking and risk exposure looks like.

A Culture that Balances Risk Taking and Risk Exposure

What would an environment that balances risk taking and controls unnecessary risks look like?

In the space provided, describe the qualities of a culture that balances risk taking exposure:

Answer these questions:

Does your organization resemble any of these?

Which ones do you lack? Check them off.

The most common responses I get are as follows:

- "Good communication."
- "People leading by example."
- "Tools for employees to use."
- "A team approach to risk management."
- "A culture of positive reports."
- "A culture where we do not shoot the messenger."
- "A balanced approach to risk taking."
- "A concern that every risk has a cost."
- "An awareness about what a risk is and what it could look like."
- "Sensitivity to risk."
- "Accountability."
- "A culture where employees are encouraged to raise their concerns and issues."
- "A culture of sharing."
- "Leaders who are more concerned about the company's success, than their own success."
- "Transparency."

The Point

The lesson in taking time to identify the ideal culture that balances risk taking and risk exposure is that as a leader you must assess your company's culture and the firm's ability to afford the risks that you choose to undertake.

Here are my suggestions on what your culture should look like.

How to Generate a Balanced Risk Taking Culture

1. *Create the environment*—A risk taker-friendly environment is one where people are invited to take reasonable challenges.
2. *Forget the procedures*—Goals and outcomes always count more than strict adherence to procedures.
3. *Instill flexibility*—A flexible approach to problems permits innovation.
4. *Encourage people*—Leaders create an environment in which good people are nurtured, supported, and encouraged to build upon their strengths.
5. *Trust people*—Demonstrate that you trust them regardless of the outcome.
6. *Foster change*—A risk friendly environment sees change as good and desirable.
7. *Be reliable*—People will risk when they feel safe and can rely on the leader. The leader models the behavior you want others to have.
8. *Control the odds*—Set limits on the losses, never risking more than you can afford.
9. *Know your people*—Leaders must understand their own risk taking attitude and those of the people around them.
10. *Know your limits*—There will always be things that you want to do and cannot and things that you are not doing that you can, so you need to know the subtle difference.

10½. *You go first*—Leaders must take more personal risks than their followers.

Culture's Impact on Risk Taking

Paradox of business success:

- Enjoy and capitalize on the good times.
- In the good times, you must look for impending dangers.

In the good times, it is easy to forget about risk. Yet it is during the upswings that executives need to be most watchful for the signs of impending danger. In aggressive "can do" or "grow at all cost" forms of cultures, when bold initiatives are being set and customers are coming in the door, it is usual to silence the messenger who carries bad news about the company's strategy or practices.

Success should make us leaders nervous because it needs to urge us to identify our level of internal risk exposure. As we know, not every risk is bad, and in order to survive today, we must take risks in order to make progress. Yet we at the top of the organization are less aware of risk exposure than those closer to the trenches. Likewise, our people closer to the operations are aware of the risks that affect their area but are blind to or underestimate the exposure impact on other parts of our organization. Therefore, understanding the conditions that create unnecessary levels of risk allow us to help prevent failure, while taking advantage of opportunities.

A business cannot survive over the long-term or prosper without entrepreneurial risk taking that leads to innovation and creativity. Success can give some risk takers, especially CEOs, too much confidence to the point where they harm the company's assets and reputation, all in the pursuit of greater gains. (Read "The Mindset of the Risk Taking Entrepreneur" in chapter 6.) This is an irresistible urge in organizations

with meteoric success. Often, in a successful firm that never experienced a loss, people move toward excessively risky deals, forge alliances with others who do not have the ability to honor their contracts, or make promises to customers that are impossible to fulfill. The catalyst for this type of behavior is the rewards built into the cultural norms. These are both your overt and hidden rewards. As the rewards for entrepreneurial behavior grow, so does your risk exposure. Therefore, we leaders must also reward smart decision making through risk evaluation and assessment.

There are two relationships regarding risk in a culture. The first is the one we all know, the ratio of risk and reward. The second one of equal importance is the relationship between risk and awareness. What sinks a company is not necessarily the risks themselves but the ignorance about the potential consequences of each viable risk. If managers are aware of the risks—their source, nature, and magnitude—they can take appropriate steps to avoid or mitigate the hidden pitfalls. This ability is critical in the operational areas or front lines of an organization. The more our people know where risk resides in our organization, the quicker they can respond and react.

Risk Inherent in Your Culture

The risk of a culture without ethics is not just to the company, it is to you as a leader personally. We are now living in a society and environment where any business owner or executive can be sued for pretty much anything. Yet, we often teach our employees to cheat or embezzle based upon our company policies. These policies can drive employee behavior in ways that we never expected.

Your employees' tendency to take advantage of you through unwarranted risk or fraud can be described on a normal distribution curve.

- 5 percent to 10 percent of your employees will never do anything unethical or be rash.
- 5 percent to 10 percent of your employees are always looking for ways to take advantage of you.
- 80 percent to 90 percent of your employees will commit situational fraud or take unwarranted risk when it is to their advantage.

Walk in My Shoes

I work really hard putting in innumerable hours, including weekends, to meet an impossible deadline. I complete the project for you on time. I ask you for a couple of days off to recuperate and replace the time I could not spend with my family. You point out to me the firm's policy says, "Employees can only take time off for sick leave or vacation." If you were in my shoes, what would you do? Get mad? Suck it up? Get back to work?

Guess what I (and most of your employees) will do? I will either take time off telling you I am sick (even though I am not), or I will come to the office but not really work for a few days.

You probably feel that I should be fired for this unprofessional behavior. But because you have chosen, as my supervisor, to stay rigid on the policy and not give me any consideration for the extra effort I put into your project, you placed me into a situation where I chose to default to my own ethical values.

Unfortunately, we cannot expect ethical behavior from our employees unless we executives and leaders model ethical behavior first. You must walk the walk and talk the talk in fairness, equity, and ethics every day. Unless you live up to the highest level integrity, you will not be able to demand this of anyone else in your organization.

Summary: Importance of Step 3

A risk management program is an attitude more than a written document. The heart of the attitude is the firm's corporate culture. However a culture is often neglected, ignored, or overlooked by leaders of business organizations. That is why we spend so much time understanding what a culture is and how it affects risk. Risk starts with the firm's strategies, which are the tools that the firm's leaders develop to carry out a business model.

In step 3 of your risk management plan, you must spend time understanding the components of the cultural mosaic and the risk inherent in those strategies, and then use this information to identify specific risks. Once you have identified the risks, you apply the tools in this section to determine the level of their impact. After you have identified this, then the firm quantifies the amount of money that needs to be dedicated from your three budgets to help mitigate or cover the cost of those risks.

This step is ongoing and is never completed because of the nature of the firm's global strategies—they are always changing and evolving. This aspect of the firm's risk management plan changes and evolves as well.

8

Step Four—Minimize the Risk Exposure

Small issues swell into huge problems when ignored.

After completing this chapter, you should be able to

- apply the three specific tools to help strategize and minimize the negative impact of a major risk.
- develop some specific ways that people in your organization can be proactive in minimizing the negative effects of risk.
- understand why risk taking requires employees to think for themselves.
- begin to delve into the real cause of a major risk.

Because avoidance of risk is not possible, it is better to be proactive in minimizing any negative or costly consequences of innovation, creativity, and coloring outside the lines.

This chapter, step 4, gives you the tools to do that. If every employee within your organization knew how to use these tools to mitigate the risk of success, you would have a healthy company with a viable future.

Risk Mitigation Tools

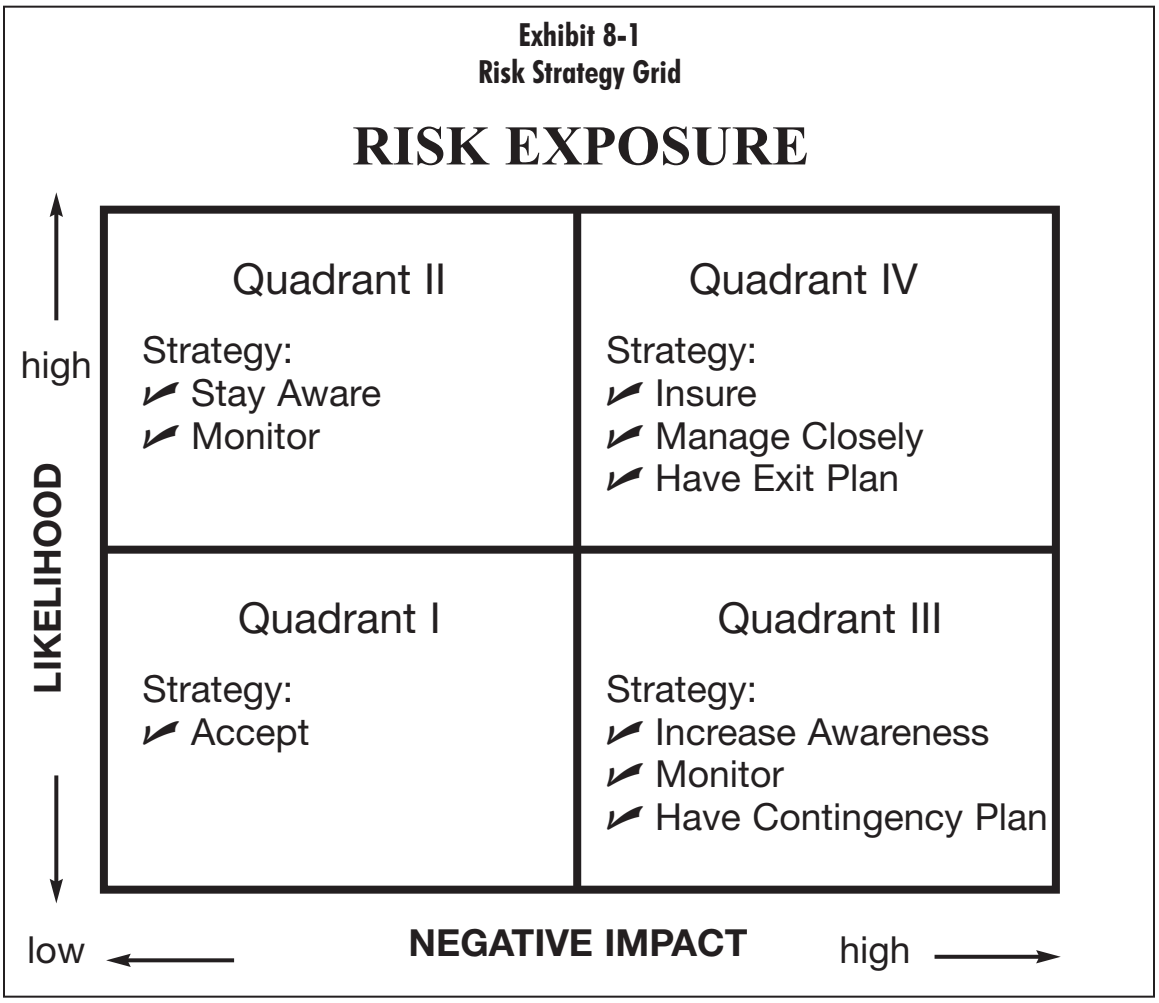
At the beginning of this book you were asked to think of a particular risk that your organization is undertaking. You now can define the optimal strategy to use based on where your exposure falls in the matrix in the following exhibit. This tool helps you to quantify risk based on two variables—likelihood and negative impact.

Exercise: Risk Strategy Grid

Instructions

Recall the risk your firm is undertaking. Define your strategy based on where your exposure falls into the grid in exhibit 8-1.

Exhibit 8-1
Risk Strategy Grid



This risk strategy grid is a common matrix that is often used to assist decision makers to foster smarter decisions. It applies to effective risk management as well.

Let us refer to the risk exposure of opening a sales office in Russia. Your main concern is the finances of your firm, because opening the sales office will tie up a big chunk of capital and you need an immediate 30 percent return on investment (ROI) to counter that risk. After careful analysis of the decisions and its impact, long- and short-term, you decide that the negative impact on your finances is low and the likelihood of this new operation turning sour is very low. This places your risk in quadrant I, and your optimal strategy is *accepting*, meaning that your leaders recognize that there could be some problems, but are committed to not letting them stop their plans.

Alternatively, if this risk means that the negative impact on your financial situation is low and the likelihood is high of not obtaining the immediate 30 percent return, your strategy will be in quadrant II of *staying aware* and *monitoring*. Monitoring any risk is critical but especially when the downside is costly.

Possible solutions are that you institute an incentive for the store's manager that fosters day-by-day awareness of some of the things that could occur or go wrong and make sure the manager believes in Murphy's Law. In the U.S., you designate specific people assigned to look at the selected metrics daily to ensure that everything is going according to plan.

If opening this store in Russia is one where likelihood of not obtaining the immediate 30 percent ROI is low, but the negative drain on your cash position is high, then you would adopt a strategy in quadrant III of *increasing awareness, monitoring*, and most importantly *having a contingency plan*. The awareness and monitoring are the same as in quadrant II, but it is at a higher tension level. You believe that it could be costly, so you make sure everyone knows that if this venture is not managed properly, the entire company can be in trouble. Your contingency plan is to create a reserve fund, or to prequalify a Russian partner that you could offer partial ownership to, or to send the best American manager to run the Russian store.

Finally, the most costly risk is the one that falls into quadrant IV. This venture, if it turns worse than anticipated, has both a high negative impact and the high likelihood of failure. Because we elected to take the risk, we adopt specific strategies equal to the level of risk. Those strategies include *insuring, managing closely*, and most importantly, *deciding on an exit plan*.

Failure to have an exit plan can come back and bite you! Some organizations continue to dig themselves into a deeper hole in that the leaders refuse to believe that failure can happen. The belief that "failure is not an option" worked fine for Apollo 13, but I know very few shareholders who support executives that throw good money at bad opportunities. There were a lot of dotcoms that became dotbombs whose only business model was to set up a company then have an initial public offering so they could cash out as millionaires. When their business model proved to be worthless, they did not have any alternatives lined up.

Answer this question:

How can this tool help to reduce the negative effects of undertaking your significant risk?

That leads us to risk management principles 7–8:

- The negative impact of risk taking is greatly reduced when you analyze the real cause of the undesirable results.
- Because you cannot control all risks, it is much healthier to be prepared for the worst and expect the best.

Proactive Attitudes

Let us explore some specific ways that you can be proactive in minimizing the negative effects of risk.

What are practical ways to be proactive toward exposure to the negative impact of risk taking?

Compare your answers with the list that follows:

Ways to be Proactive in Minimizing Negative Effects of Risks

☐ *Check your ego at the door.* Leaders with a strong belief in themselves and their ideas can easily impose their will on others.

☐ *Keep asking, "But what about …?"* In today's changing environment, there is a fine line between being decisive and being blind.

☐ *Nobody is as smart as everybody.* Many leaders fail to involve others in their strategic decisions. If you want visionaries, you must first build visionaries.

☐ *Simple mistakes do not have simple causes.* Simple mistakes often involve more than one person, which means you are facing group dynamics or cultural problems.

- ☐ *Little mistakes yield big insights.* If we act a certain way with the small things, we will act the same way with the big things.
- ☐ *What gets measured gets monitored. What gets rewarded gets repeated.* What are you measuring and why? What are you rewarding and why?
- ☐ *Wake up.* Leaders must influence people to consciousness about risk's reality.
- ☐ *Assess your risks.* Set a valid basis for your decisions.
- ☐ *Inspire people with your internal control system.* Controls must not be made to prevent action, but to allow people to take it.
- ☐ *Information is the "Breakfast of Champions."* Help people to know what information is needed and why.

Check off all those that you are currently practicing. (Be honest!)

Importance of Step 4

The essence of step 4 is to minimize your firm's risk exposure or better yet to inspire actions to lower the cost of failure. The next part of your risk action plan is to perform an authority and responsibility analysis.

An underlying purpose of an effective risk management program is to foster constant awareness of everyone throughout your organization about risks—large and small. Leaders, all too often, make a mistake that is detrimental to fostering awareness. As managers and supervisors, we give employees the responsibility for something yet fail to give them the authority to take action. In proper risk management, when we asked people to be accountable and empowered about doing things to reduce risk or its cost, we must be 100 percent sure that we have given the specific authority equal to that responsibility.

Disempowerment Inaction

This happened to me recently:

I am leaving the next morning for an out-to-town consulting project. I stop at a large office supply store chain to get some hard-to-find protective covers that I use for documentation purposes. I find only one box of 50, but it had been opened. I search around but cannot find other boxes. I take my purchase to the counter and show the clerk the torn box and ask her if she can locate another box. She checks and says, "No, that is our last box." I express my concern that there could be some protectors missing so she counts and finds only 49 sheets. At that point the sales clerk does not know what to do next.

I am anxious to get going because I have several things to do before I call it a day. She is the only cashier and now several customers wait impatiently behind me. Because the clerk is at a loss she calls for a manager. We wait and we wait. I suggest, "Just deduct 5 cents from the box price to cover the cost of the missing protector." She replies, "I'm not authorized to give any discounts." We wait and we wait. That evening the office supply store chain created much ill will, not because of 5 cents, but because their culture is one where employees are not allowed to think for themselves.

Employees Who Think for Themselves

Compare my example with the Marriott Hotel group. Marriott has a policy for all its frontline employees: "You can spend up to $2,000 to satisfy any customer problem." There are five questions that Marriott employees must answer to themselves before they give or spend money to solve the problem. The five questions posed to employees are as follows:

1. Will this action harm the reputation of the hotel? ____
2. Will this action cause a problem for another guest? ____

3. Will this action only defer a problem? ____
4. Will this action upset the guest even more? ____
5. Is this action illegal or unethical? ____

If the answer to all five questions are "no," the employees can take the action they deem necessary to satisfy a guest or a customer.

What Marriott has learned from their empowering policy is that it usually takes somewhere around $100 to satisfy the customer or solve the problem. It might be buying the guest a meal, picking up the cab fare somewhere, comping one night's stay at another hotel, or providing a gift such as a bottle of champagne or wine. Rarely, if ever, is the entire $2,000 spent.

Answer this question:

Do you trust in your employees enough that you would give each of them $2,000 of company's cash and trust them to only use it to save a client relationship without going to someone for approval?

If you are like most people, fewer than 25 percent would feel comfortable doing this! If you are among the 75 percent who feel uncomfortable, then your firm, like many organizations, is unable to equalize responsibility with authority. This type of culture will undermine an effective risk management program.

Balanced Risk Taking Requires Employees Thinking for Themselves

I did a session on this topic in Reno, Nevada, and one very wise woman summarized the importance of this need to equalize authority with responsibility. She did not give her name, so I cannot give her credit for this astute observation. She told the class:

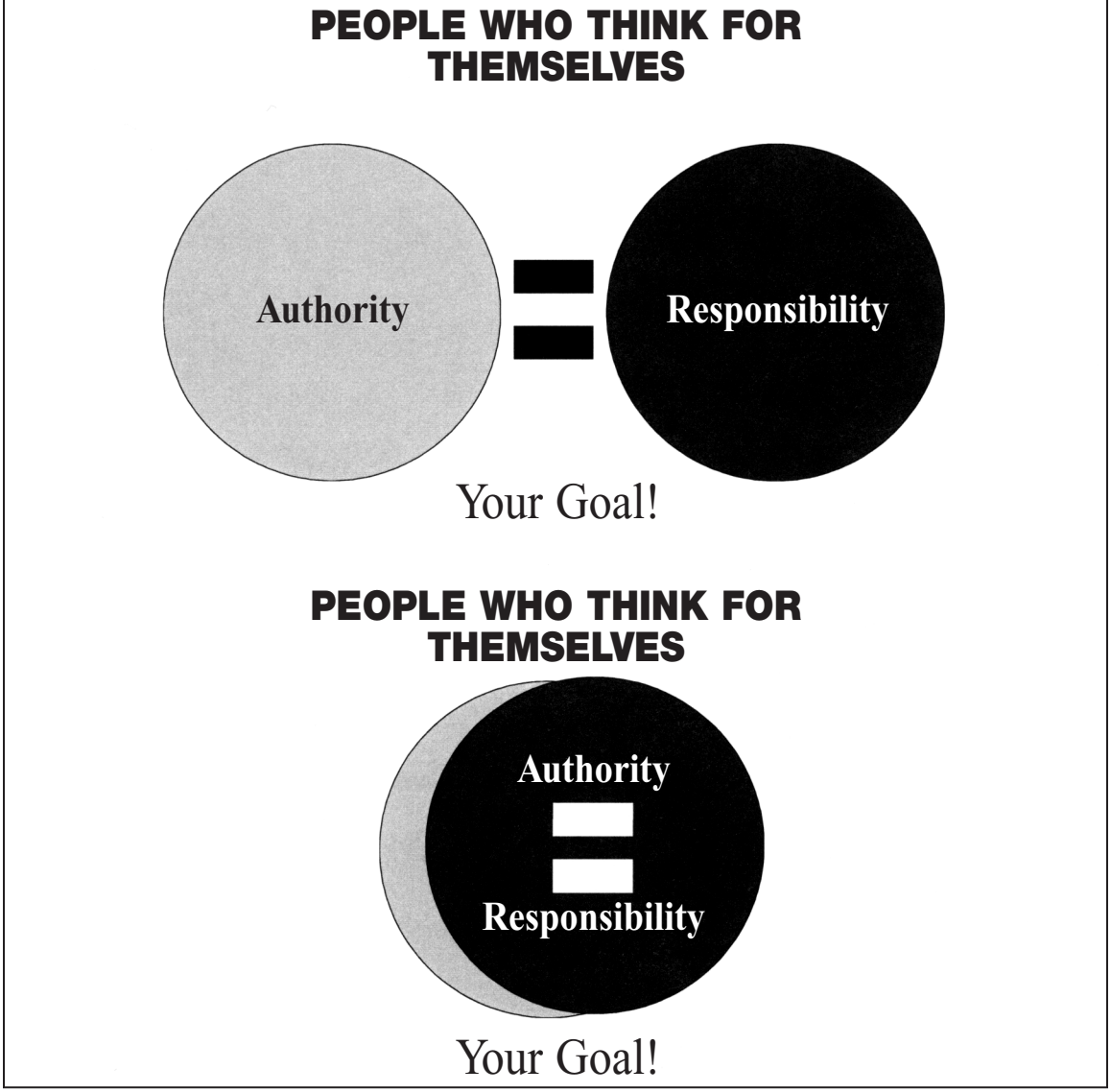
"If you make employees responsible for unlocking the door, give them the key!"

In your organization, you are asking employees to monitor for risk—asking them to unlock the door—but you are not giving them the tools, the knowledge, or the authority to do something about the risk. You and other leaders refuse to give employees the key to the door!

A risk management program requires employees at every level, who are making decisions and taking action, to let leaders know when there is something going wrong. Employees need to believe and know that they will not be punished for blowing the whistle or waving the red flag. That is why we leaders need to strive to match authority with responsibility so that employees can and will think for themselves.

In exhibit 8-2, you will see the two circles coming together. Your goal is to try to match them up as closely as possible. You will never get it to be a 100 percent match, because of the need for internal control affects empowerment and authority. These checks and balances need to be seen as empowering employees to take action and not as impediments.

Exhibit 8-2
Matching Responsibility with Authority



Tool to Perform an Authority and Responsibility Analysis

Answer these questions:

Where have you defined each decision maker's authority to represent the company?

How is it communicated?

How is it updated to reflect change?

Does the average employee know of its existence or even its contents?

Do you use any type of authority or responsibility chart? How does it work?

A tool that will allow you to equalize responsibility with authority is called a risk authority and responsibility chart (RARC). You will notice in this tool that you can easily highlight specific areas of concern, in this case, internal control over actions and decisions. This tool was used by a Seattle organization where I was controller. This is one page from a series of RARCs and was directed toward the controller's team. I supervised the accounting manager and the credit manager. While I reported to the president, I had a dotted line relationship with the vice president of finance of our parent company, whose office was in New York City.

Exhibit 8-3
Risk Authority and Responsibility Tool

Authority and Responsibility Chart	*Accounting Manager*	*Credit Manager*	*Controller*	*VP of Finance*
Set policy	R	R	R	A
Finalize procedures	A	A	I	I
Hire from outside	R	R	R	R
Hire from inside	R	R	R	A
Institute compensation programs	R	No	R	A
Make purchases and expenses:				
Normal supplies	$100	$300	$5,000	$50,000
Expense reports	$100	$100	$1,000	$2,500
Travel plans	No	No	A	A
Capital equipment	R	R	R	A
Credit memos:	R	A	R	R
Adjustment to inventory	R	R	A	R
Write-off inventory	R	No	R	A
Price adjustments	R	No	No	R
Adjust customer Accounts Receivable	$100	$25,000	$50,000	No
Issue special customer terms	I	A	I	I
Public relations:				
Speak for company	No	No	No	R
Issue press releases	No	R	R	R
Security:				
Alarm system access	Yes	Yes	Yes	Yes
Computer system access	Yes	Yes	Yes	Yes
Warehouse access	Tour Only	No	Yes	Yes

Legend

$	Dollar amounts show maximum approval limits per event
R	Recommend
A	Approve
I	Be informed

The chart uses three symbols signifying authority and responsibility: the *R* means that the person could recommend the action; the *A* means that the person has the authority for the action; and *I* means the person is to be informed. Remember, even though it is your job to keep me informed, it is my job to stay informed—communication is a dual responsibility.

Notice (on the chart) that the accounting manager, credit manager, and I can recommend a policy, but final approval and authority rests with the vice president of finance. This makes sense because the vice president has a concern for the big picture. When adopting procedures, the actual people doing the work (the credit and accounting managers) have the authority to make it happen. Their responsibility also included keeping the vice president and me informed.

Look at the structure for the issuance of credit memos (halfway down on the chart). One reason I was selected to be controller for this organization was because of a huge problem with inventory adjustments. Every year for the prior five, the book inventory had to be adjusted downward, and nobody could find the source of the discrepancy. What I found was that "everybody and their brother" could make general ledger (GL) adjustments to our book inventory. My first action was to clamp down and stop these entries. I used this tool to create restrictions on who could make adjustments to our GL inventory. Notice that the accounting manager and credit manager could recommend inventory adjustment entries, but required my approval. Even the vice president could not adjust our inventory. Before I changed this, both the credit and accounting managers could adjust inventory without restriction. I wondered what reason they would ever have to make journal entries adjusting the inventory. With this control in place, now I would know.

For the decision to write off inventory, the accounting manager could have reasons to recommend the write-off, but I could not see any reason why the credit manager would need to. In fact, I felt that would be a conflict of interest for him to the make inventory cost or valuation adjustments.

Similarly, when it came to adjusting specific customer accounts, I limited the accounting manager's authority to $100, which would cover immaterial things like deductions or charge backs. My credit manager could adjust a customer account up to $25,000, and if the issue was larger, he would come to me. If, in the rare instance the inventory adjustment entry was more than $50,000, we needed the CEO's approval. Notice that even the vice president (located in New York) could not adjust our customer accounts.

Sarbanes-Oxley Compliant

This is a tool used by many organizations in some form or another. Best of all, it helps you meet your Sarbanes-Oxley documentation requirements.

One way to make this tool even more effective is to have it online on the company intranet. Then, if employees or managers want to understand what control procedures are involved in an action or decision, they click on the hyperlink and go to the Web page where you have that information. Also, let us say that you decide to increase your accounting manager's purchase authority for office supplies from $100 to $1,000. You can do that quickly online. This tool gives you flexibility, while defining and communicating authority and responsibility and developing control awareness over risks.

Answer these questions:

How would this tool help your organization decrease the negative impact of risks that you undertook?

How will this tool decrease the negative impact of risks?

How will this tool increase accountability in risk taking?

Tool to Analyze the Causes of Exposure

This tool, known as the *Five Why's* allows us to find the root causes of risks that can lead to detrimental effects. The cause of the downside of risk taking is rarely in the physical things like bricks, mortar, or tools. Most of the time they are generated or caused by how people think and act.

To understand how this tool works, I use an example (this actually occurred in a company where I was controller) where an empowered product manager purchased products that he felt we could sell. Because we emphasized to all our purchasing folks that they needed to use their best judgment when dealing with the vendors and making purchasing decisions on their product line, they almost always had the final say. We thought we had in place clearly defined policies. We found out that this was a false assumption. Our product manager obligated us for a product that later did not sell and, as we discovered later, was not returnable.

The Five Why's has four simple steps, but do not get fooled by its simplicity. It is the questions that you keep asking *after* you get your initial answers that makes it so powerful. As financial officer or executive, our task is to find the root cause of a problem. We often waste so much time on finding and removing the smoke that we never get to the cause of the fire. This tool allows us to discover what caused the fire so that we can prevent the fire from starting again.

Steps of Five Why's:

1. State the risk as a problem.
2. Ask: "Why is this happening?"
3. Continue to ask why until you get to a root cause that (*a*) you can do something about, and (*b*) when reduced or eliminated, the situation will change for the better.
4. Summarize your findings.

Example of a Risk Exposure

Using the decision making tool called Five Why's, let us try to find the root causes of a common and specific exposure to a risk.

Statement of Problem

Empowered product manager obligates our company for a product that does not sell and is nonreturnable.

Now that we know the problem, we ask the first question:

1. Why did this happen?

   The manager did not adhere to the company's policy for acquiring a new product line.

We discover through investigation that the manager did not adhere to the company's policy for acquiring a new product. Our policy in part states, "A product manager may not agree to purchase a product or product derivation that is designated by the supplier as nonreturnable ... Any exceptions must be approved in advance by the vice president of operations."

Normally most of us would stop at the first why and would fire that product manager for violating a policy. If we do that, however, all we have accomplished is to deal with the smoke and failed to search for the cause of the fire. So by being good, astute, and smart people, we want to prevent the fire. We ask again:

2. Why did this happen?

   The manager wants to impress the vendor.

Maybe it was a new relationship or something similar. But we find that this product manager agreed to this contract based on the personality of the vendor.

We proceed to ask again:

3. Why did this happen?

   The manager is looking for something above the ordinary.

We find several instances in our research that this manager has done this before—seeking out special conditions in his initial dealings with other new vendors.

Let us review ethical implications. As a CFO, controller, or auditor who is concerned with the ethical attitude of this person, you would jump up and down and demand this employee be fired. But you do not know if this situation is an isolated event or might be happening with other people in the company.

Back to the tool, you ask again:

4. Why did this happen?

   The manager wants to get paid his large incentive bonus.

You uncover that the manager wanted to get paid his large semiannual incentive bonus.

Aha! Now we are starting to get to the root cause. By using this tool regularly, you will find the root cause is often based around power, emotion, drive, greed, or lust. Some human frailty is involved with lingering problems, especially those related to unwarranted risk taking and ethical breaches.

We ask again:

5. Why did this happen?

   The incentive rewards employees for increasing the product line and does not penalize them for inventory that does not sell.

We discover that the incentive program for all product managers was designed for them to expand the product line's diversity. The incentive contains no penalty or downside for inventory that does not sell. Whoever set up the incentive felt the need for people to bring stuff in the door, but failed to hold them responsible for the stuff once it is on the shelf.

Again, we could stop there, but your intuition tells you there could be another cause for the fire.

You do not have to stop at five why's; you can go on with as many as possible, but usually five or six is enough to get to the fire's cause.

6. Why did this happen?

   The emphasis on managing inventory levels and turns is seen as a function (responsibility) of the inventory control group, which reports to the controller. The product managers report to the operations manager.

The responsibility and the controls over managing inventory levels and inventory turns are viewed as accounting's area of expertise. This key control function has been given to the inventory control manager, who reports to the controller. The product manager reports to the operations manager, a function completely outside of accounting.

Answer these questions:

In this example, what do you see as the real risk?

Now that we know the cause, what can we do to affect it? In other words, what needs to be done to prevent the fire from happening again?

The Real Risk

What we discovered in using the Five Why's tool is that we split the authority with responsibility. We made the purchasing group accountable for the purchasing side of inventories and made accounting accountable for the control side of inventories. By not paying attention to what behaviors we reward, we split responsibility and authority!

The lesson from this tool is that once we find the root cause for the possible negative impact of risk taking, we can take smarter actions to reduce the negative impacts.

Exercise: Finding the Root Cause

The following is a blank form listing the Five Why's for you to use. As before, you are encouraged to think of specific risks or problems and go through the Five Why's and conduct interviews to discover why your problem or risk is a reality.

Instructions

Following the example on the previous page and using Five Why's, try to find the root cause of one of your firm's specific exposures to risk.

The Exposure:

1. Why could (did) this occur?
2. Why could (did) this occur?
3. Why could (did) this occur?
4. Why could (did) this occur?
5. Why could (did) this occur?

Conclusion:

What seems to be a possible root cause of your risk exposure?

Tool for Isolating the Optimal Solutions

A tool called a Criteria Checkerboard allows us to analyze the exposure of a specific risk and then use the information to determine how to proceed. It is a key tool used by consultants for defining and matching the criteria for success with the possible alternatives. Using this information, you can analyze your exposure to a risk and then use the data to decide the best solution or path to take.

Steps for the Criteria Checkerboard

1. Select your criteria for a best decision
2. Brainstorm alternative solutions
3. List the criteria and alternatives on a checkerboard
4. Check off how well each solution meets your criteria

Example of a Risk Exposure

Your information system is vulnerable to sabotage by outsiders.

Which of your plans is the best solution to reduce the exposure?

We will walk through the tool by using an example of our exposure.

Our existing (and very old) information system is vulnerable to sabotage from outside the organization. Your leaders made a risky decision to spend a pool of funds to generate sales using the Internet, leaving insufficient funds to upgrade your current technology. You, the controller, informed the leadership team of your concerns. They instruct you to recommend the most viable and optimal solution within these three specific constraints:

1. The fix must make your system invulnerable.
2. The fix must not cost a lot.
3. The fix must be easy to implement without adding any people to the IT staff. (I know that if you were in this position, you would turn in your resignation immediately because they just placed you in a no-win situation, but stick with me so you can see how this tool will help you out of your job security problem as well as dealing with the risk!)

Because your leaders have increased your firm's exposure and therefore your risk, you need to find an optimal solution to lower the cost of vulnerability. You also need to find the best solution out of a series of options. (And show the leaders that their restrictions are unrealistic.)

The first step of the tool is to select specific criteria for the best decision. Then, brainstorm alternative solutions that cloud possible work to solve the problem. Next, list our criteria and alternatives on the checkerboard. Finally, compare how well each solution or alternative fits into the criteria.

The key part is selecting the specific criteria. Your criterion decides what will make a good decision so that you minimize the risk's impact. This is always your starting point. Our leaders gave us three things they wanted:

- Make our system invulnerable
- Keep the cost for additional security low
- Find a solution that is easily implemented without adding staff

Next, once you have the criterion, and before you determine whether the criteria are valid, you select some alternatives or potential courses of action. In selecting alternatives, you want to use the rules of good brainstorming. This means that every idea is acceptable and possible, and no ideas are too outrageous. You write down every idea as it is presented. You stay open to the idea no matter what the source or the rationale for it.

Our solutions team brainstormed several ideas, including the following:

- Disconnect from the Internet
- Monitor the system 24 hours a day, 7 days a week.
- Outsource our entire IT function.
- Employ a high-end firewall.
- Require that employees change their passwords weekly.

Possible Alternatives	*Criteria 1: Makes system invulnerable*	*Criteria 2: Keeps cost for security low*	*Criteria 3: Is easily implemented without adding staff*
Disconnect from the Internet			
Monitor the system 24/7			
Outsource our IT function			
Employ a high-end firewall			
Change passwords weekly			

Later, you go back and narrow the list down to the more reasonable or realistic alternatives. In this example, we already narrowed down (through the rules of good brainstorming) four viable alternatives. Now your job is to go through the checklist and compare all the alternatives with your three criteria or restrictions.

You will notice that the only alternative that meets the restriction of "make our system invulnerable" is to disconnect from the Internet. Yet we need access to the Web to do business. Now you have proof that your firm's executives know nothing about technology. So we toss out that criterion.

You will notice that the restriction of "low cost" is too vague. This needs more definition.

You will also notice that alternatives "employ a high-end firewall" and "change passwords weekly" can be combined into one.

You know, of course, that outsourcing IT has severe repercussions and is not something you do just to avoid someone getting into your system. While it meets criterion 3 "no more IT staff," there is no guarantee that your IT service vendor's system will be any less vulnerable than yours!

After further work, your team arrives at an alternative that meets most of the executives' concerns.

"Implement a complete security plan that includes changing passwords monthly, increased monitoring, employing a high-end firewall, and training employees on security issues every month."

Now that we applied the tool, answer these questions:

- *How will this reduce our exposure to the negative consequences of having a vulnerable information system?*
- *Which of these alternatives meets our need for "Best Solution"?*
- *Why is it optimal?*
- *How would this reduce our exposure to the negative consequences of having a vulnerable information system?*

The lesson from this is that because every risk has a cost, it is important to use decision making tools to uncover these costs and possible negative downside.

Summary: Importance of Step 4

Once we have convinced people in the organization that there is a risk that we need to treat seriously, step 4 starts us moving toward taking action and placing tools in the hands of employees, so they make smarter decisions. There is an old saying, "Fully warned is fully armed." Except for strategic risk or faulty assumptions in the business plan, it is rare that an executive identifies a particular operational risk. It is almost always an employee who is doing the work and dealing with the situation who recognizes a cost we cannot afford. Our job as leaders is to help the employees at this level define the seriousness of the problem, so they can take action.

9

Step Five—Recover From the Negative Results

Risk Happens!

After completing this chapter, you should

- understand how a contingency plan works.
- be able to prepare a pitfall analysis.
- be able to develop a lessons learned program for your team or company.
- recognize and explain the importance of the risk management audit.

Despite our best planning, anticipating, and analysis, Murphy's Law still exists. There will always be things that we cannot anticipate, or our implementation goes awry, or we make human errors in judgment. Yes, even leaders can be wrong. I believe every entrepreneur, CEO, COO, and CFO should have the statement "Risk happens" tattooed to their foreheads so they can see it every day.

An imperative in your risk management plan is created where employees within your organization have a specific methodology for recovering quickly from a negative result. The key element in this step is to make sure that you hone your recovery skills on the small lapses.

For example, say that you get the itch to run a marathon. You are not a runner and have never run one before. Instead of going out and immediately trying to run 26 miles, health experts will tell you that you prepare by taking small steps. Your first task is walking and setting a milestone of being able to walk two hours without stopping. Next you alternate walking and jogging until you can go a mile without stopping. Your next task is to build up stamina until you can run that mile without walking. When you are comfortable with a mile, you extend it to two miles and then three miles. You continue with these smaller goals until you are able to run more than 26 miles in one outing. Can you do this in one day or even one month?

Of course not!

The same holds true for good risk management. We must use the same tools and methodology on smaller, less costly risks, so when a larger risk crops up, one that has a terrible cost of failure, we can face it with confidence. Soon, your firm will have the ability to recover quickly no matter what unexpected things occur. Like any muscle in your body, the more you use the muscle, the stronger it becomes. Similarly, the more you practice risk management in your day-to-day decisions, the stronger your program becomes.

Here is a good example that likely hits close to home. I'm sure that your firm has a backup mechanism for your information and data collection system. I am also sure that no one in your firm has thought to have a dry run of that system.

We assume that the backup system works because it collects and mirrors the original data. But we riskily assume that when the unthinkable occurs, this backup system will take us back to the point before the failure. Mr. Murphy is laughing at those of you who believe this! The only way to know for sure is to actually crash your system several times and jump start with the backup system.

No one wants to tackle all that work of verifying each data point because of the time and effort it will take to do so. Why are you accepting this clearly identifiable risk?

Risk Recovery Tools

The more you practice risk management in your day-to-day decisions, the stronger your program becomes.

Tool for Pitfall Planning

The tool for helping you to recover quickly is a pitfall analysis. Financial folks automatically think in terms of pitfalls and coming up with alternative plans—it is our way of life. I am here to tell you other people (that is, nonaccountants) do not. This tool works for not only us planners, but works well for people who normally do not think long-term or analytically and critically. This tool forces them to think that way. Using this decision making tool, we can create ways to learn lessons from exposure to a risk.

Steps of Pitfall Analyzing

1. List the possible pitfalls of a particular course of action.
2. Create contingency action plans for each pitfall.
3. Determine what would prevent implementing the plan.

An example we will use to understand this tool is one that we have all experienced and one fraught with exposure: converting to a new accounting software platform. Assume that this is a major upgrade. You have been using a middle-market type of software and decide to go big time and invest in a million dollar real-time database platform. For those of you who have gone through one of these, you know that this conversion is a minefield.

In this example, assume the following:

You, as a lead on this project, identify these potential and common pitfalls:

Pitfall	*Contingency Plan*
Losing a key member of the conversion team, especially Dan or Dana.	Hire qualified temporary for length of conversion project to support Dana and Dan.
Conversion process takes longer than expected.	Spend more time planning up front and hold weekly update meetings with conversion team.
Cost of conversion is more than the budget established three years ago.	Prepare an updated cost projection with help of consultant. Request budget update meeting with CEO ASAP.

Answer this question:

How would this tool help you to minimize the negative effects of the exposure and recover more quickly?

Exercise: Pitfalls of Risk Taking

Instructions

In the space below, you have an opportunity to think of risk that you, your team, or your firm is facing and list the potential pitfalls and your recommended contingency plans. Do not forget that contingency plans also include allocating or budgeting money to spend for that particular problem. There is a prevailing belief in budgeting that using contingency funds is a bad thing. There are risks, but if they are handled correctly, you can turn them into a positive aspect and an asset to your risk management program.

Describe Your Exposure:

Potential Pitfall	Suggested Contingency Plan
1.	
2.	
3.	
4.	
5.	
6.	
Is there anything that can prevent you from undertaking these plans?	

Contingency Funds in Risk Management

Let us go back to your exposure of opening a store in Russia. For the next year, as you expand your presence there and establish a beachhead, you include in your current year's budget a contingency fund of $50,000. This $50,000 can only be spent under three conditions:

1. If the sales in Russia fail to reach $2,000,000.
2. If the potential customers do not become aware of your product, based on an independent survey.
3. If the method of advertising through the most popular newspapers proves ineffective in attracting consumer attention.

Only if all three conditions are met can the $50,000 be used to hire sales agents to sell your product and offer cash-back incentives to storm your way into the marketplace. Now if during the year only one or two of those conditions are met, this fund cannot be used, even if sales continue to look bleak. This contingency fund cannot be used for any other purposes, such as bailing out the Seattle stores because the manager there is inept and you will not earn your incentive bonus because of him.

If these three conditions do not happen in the current year, then you carry the contingency fund over to next year. You can maintain or modify the conditions under which the dollars can be spent.

This is how to properly handle a contingency fund. After a certain point of time—say the Russian stores meet all sales, profit, and ROI targets—the funds can then be returned by reversing the contingency expense, thus adding to the current year's profits because of good management.

When we take the time to look for pitfalls and then develop contingency plans in advance, we grow in confidence in our ability to face or accept more risk.

Tool for Fostering a Lessons Learned Attitude

Another way to help build up your muscles for recovering quickly is to adopt a lessons learned program into your cultural norms. It needs to become a critical part of your culture mosaic. All organizations with effective risk management programs use this technique, though they may refer to it in different terminology. Yet, consistently, firms that are proactive in quickly identifying and mitigating risk rely heavily on their lessons learned from risks taken.

Answer this question:

What kind of lessons learned process does your organization have?

That leads us to the next truism.

> Risk management principle 9:
>
> - It is much easier to recover from negative impact of risk taking and unexpected challenges when you have taken the time to learn from previous challenges.

Your lessons learned in step 5 not only foster dialog and force cross-functional communication, they also help us to see risk holistically as dictated by the Committee of Sponsoring Organizations of the Treadway Commission and Sarbanes-Oxley.

The lesson in this tool, a critical step in the risk management plan, is to learn from our mistakes and *successes*.

Exercise: Lessons Learned

What have you learned from your organization's mistakes and the risks you have undertaken?

The Risk Audit

Effectively managing the risk of doing business is becoming a critical driver in many companies' success or failure. Taking a comprehensive view of your risk management strategies periodically through an audit or formal review process is a good way to learn from your successes and misses. This risk management review is an opportunity for the company to assess its ability to both handle risk and to recover from its downside. The key element is to make sure that you are actually learning something so you see improvement over time. For example, an acquisition, a merger, or the significant change in accounting policy within the company can significantly change your organization's risk strategy.

Ongoing Protection

Think of managing a risk as protecting your personal computer from a virus. A virus can come through many different forms. So you establish a firewall to prevent viruses from coming through your ISP. But do not forget that viruses can be attached to documents that are in purchased software or when someone gets into a computer system through an employee's unprotected home terminal. Even worse, someone could send you what seems to be a harmless E-card that contains a virus, which is not detected by your firewall. Even if you have the best firewall available, you must update it regularly and run a daily check for new viruses to make sure that the tool is doing its job.

The same holds true for your risk management program. You could have strategies and tools in place, but that will not always prevent a costly risk from affecting you, especially if it comes from left field, like one caused by a foreign government or by a strategic partner who has nothing to do with you. Just as you update your firewall and run a daily protection scan, you must also regularly review your risk program by updating your strategies, examining your plans, and conducting a risk audit or review.

A risk audit will help you to know if your risk management program stays in alignment with your company's overall strategy and objectives. The goal is to make risk management review a part of your everyday business. You can use this review process to strengthen long-term relationships (and hopefully reduce premiums) with insurance brokers and underwriters.

As you gather information from your periodic risk audit, this information will be helpful in negotiating with underwriters. Resist the temptation to tie the timing of this review to the purchase of your insurance. The goal of the review is to identify the weaknesses in your system of controls regarding risk identification, oversight, and mitigation. More than likely, you will find in your review that your company has retained a certain risk unintentionally, either through benign neglect or lack of internal communication.

Risk Audit Team

Your audit team consists of people throughout the organization, including operations, accounting, IT, human resources, and any other service areas that are affected by risks such as a safety program. It is critical that this cross-functional team communicate and relate well to each other, because their charter is to ask one another: "What is keeping you awake at night beyond our normal risks?" This requires the team to think creatively, organically, and holistically at the business. If applied properly, the annual review will open employees' eyes to the impact that one risk could have on multiple departments or functions within the business.

This audit team must be headed by a senior executive who represents both the company and shareholders' interests as they relate to risk management. The goal of the committee is to develop a customized audit risk checklist so that individual managers (the actual risk takers) can assess the risk versus reward of their particular area of responsibility. The checklist asks managers to indicate their awareness and knowledge of the potential risks, define those risks, and identify how they are being addressed on an everyday basis. The key question could be: "How many resources are being spent to address or mitigate this issue?" Do not forget that the resources include people's time, extra paperwork, audits, and energy—the time that could be spent in more productive endeavors.

The Audits Findings

Once the risk review is complete, your company's next step is to use the information that it gathers to improve its overall risk management. By incorporating the review's findings into a specific plan for risk management, the company should be able to minimize the chance that the audit findings will gather dust on your shelf. It makes sense that the leader of this audit team is the chief risk officer, and part of the team's membership consists of members from the risk management committee.

Your risk audit will likely provide you with a great deal of knowledge about your current state of affairs as it relates to risk management and your overall state of risk taking. Some of this knowledge will be beneficial and welcome, while other parts of it will be dreaded and unwelcome. In risk management, knowing the good with the bad makes the organization stronger and more likely to withstand serious and unanticipated risk. It may even give you a competitive advantage and build the confidence to risk more.

Tool for Continuous Learning

The Plus/Delta analysis tool is an excellent learning tool for every meeting, project, or performance evaluation.

The Plus/Delta analysis is a summary of what is worth repeating and what needs improving. It spawns rapid improvements, shortens the learning curve, and increases accountability.

The Plus/Delta gives employees and the risk audit team invaluable insight on what to continue doing and what to change. They use this as they plan for each risky venture, during the progress and monitoring, and at the end. At each phase, the things that are working are identified (pluses) and the improvements noted.

Sarbanes-Oxley demands this sort of documentation because companies that fail due to a high risk exposure are always unable to prove the soundness of the reasons why they took the risk in the first place.

Exhibit 9-1 **The Plus/Delta Tool**	
Pluses **+** (Things that work and should be kept)	Deltas Δ (Things that need to change or be better)

Steps of the Plus/Delta:

1. Announce the purpose of the Plus/Delta.
2. Spend time gathering a list of things that worked well and list them on the "plus" side.
3. Spend time gathering a list of things that people would like to see changed and list them on the "delta" side.
4. Before the next session or committee meeting, address the changes that were recommended and accommodate those that cannot be changed.
5. Start the next meeting by reviewing the most recent Plus/Delta.
6. Remind the group that you will continue doing what worked.
7. Inform the group of the changes that will come from the list.
8. Explain which changes cannot be implemented, and brainstorm alternatives.
9. Continue to use the Plus/Delta tool at each meeting, event, or gathering.
10. Notice and celebrate how quickly improvements are taking place.

Note: This is good documentation to retain for demonstrating to others that you are being proactive in addressing risk (an insurance premium benefit) and are in compliance with Sarbanes-Oxley.

Case Study

Analysis of Wal-Mart's Growing Risk

Despite its success, Wal-Mart is a very large target for many. One example is that two union-backed groups have formed a shared mission to challenge the retailer's record on business, labor, environmental, and social standards. One of these organizations named WakeUpWalMart.com has set a goal of trying to reform Wal-Mart.

To understand the size of Wal-Mart, if Wal-Mart were a country, its economic output would place it as the twentieth largest country in the world. According to CEO Lee Scott, Wal-Mart employs 1.2 million workers and pays an average wage rate of $9.68 per hour.

Wal-Mart is also currently being pressured by states that are trying to force employers such as Wal-Mart into improving health benefits. The states are publicizing the names of companies that have the most employees enrolled in their public health programs.

Recently, a leaked memo from a Wal-Mart benefits executive suggested that the retailer could lower its healthcare costs by screening out unhealthy people from working at its stores. To counteract these criticisms, Wal-Mart is doing many things including raising the CEO's visibility by having Scott travel and speak throughout the United States. In addition, Wal-Mart has doubled the number of Washington lobbyists it employs and increased its political spending. Wal-Mart spent $1.5 million in its lobbying efforts in the year 2002 through its political action committee. In 2003, Wal-Mart spent $2.2 million. Notice how Wal-Mart chooses to mitigate its reputation risk.

The lesson here is that even if you are a success, you run the risk of people and organizations resenting your success or expecting something of you that they believe you owe them. This same phenomenon has happened to Nike, Starbucks, Microsoft, Hewlett-Packard, and others. This sadly will continue indefinitely. This risk is both uninsurable and very difficult to quantify and measure.

A Business Recovery Strategy

I found an illustrative example of lessons learned in *Fast Company* magazine. The article was titled "Make Smarter Mistakes." These are six reality-tested strategies for learning from your mistakes that apply to the negative effects of risk taking.

1. *The cover-up is always worse than the crime*.—The surest way to defuse a mistake is to "fess up" and face up quickly.
2. *If it is your team, it is your mistake*.—If something bad happens in your group or unit, you own the mistake and the recovery plan. People forget the problem, but they remember your actions.
3. *Follow-up is as important as follow-through*.—Little mistakes yield big insights.
4. *Seize the moment of truth*.—Learn from the problem and its effects as quickly as possible.
5. *It pays to make mistakes*.—Even when things are going well, we need to be shaken up and tested.
6. *Sometimes the best fix is a quick fix*.—The quick solution can buy you time to learn and implement a lasting prevention.

CEO Lessons Learned

In the same issue of *Fast Company*, several writers interviewed well-known executives and asked them about the lessons learned regarding risk taking. Be sure to study these to discover that even bold risk takers realize they cannot foresee every pitfall or downside:

- James Busby of QMS—"Never risk thy whole wad!"
- Patrick Corrigan of the Corrigan Group on network systems—"Disaster recovery? We'll think about it tomorrow."
- Nikki Strange of DriveSavers—"People's fear and frustration about losing data prevents them from thinking clearly. As long as the anger is 'out-there' blaming others, it prevents quick recovery."
- Andrew Jarecki, CEO of MovieFone—"We failed to test the system before implementing a high-tech solution in a low-tech environment."
- Charles Conn, CEO of City Search—"We committed to the wrong technology."
- Jeff Bezos, CEO of Amazon.com—"We overcommitted on startup inventory."
- Orit Gadiesh, Chairman of Bain and Company—"We rushed implementation of a client project."
- Barry Keesan, CEO of WorkSmart International—"We undercapitalized an expansion of a fast-growing publishing business."

Summary: The Importance of Step 5

This step, a healthy evolution in a business, is maturity. In the prior steps, we acknowledged that the downside of risk taking exists and that it is inevitable. Now that we have this realization, employees have tools that they can use to learn from successes and failures. As in the example given about protecting your personal computer from viruses, a risk management program provides a firewall for the organization as a whole. As my beloved grandfather used to say:

"Since you ain't the brightest crayon in the box, here's my advice for you: if ya ain't learn nothing from your mistakes, then don't make any, ya' darn fool!" (You had to be there!)

10

Step Five 1/2—Commit to Taking Action

After completing this chapter, you should be able to

- rate your risk management program against a continuous improvement environment.
- create an action plan that addresses areas of risk within your firm.
- obtain written commitment from employees on what they will actually do to minimize or address unnecessary risk.

The (Never Completed) Last Step

To you, this last step may seem like an afterthought, yet it is very crucial to the success of your risk planning efforts. Even if we learn something from our lessons learned program (in step 5), unless your employees actually implement the identified changes and improvements, you waste the time spent in understanding the causes of risks and how to avoid them. Nearly every organization that has effective risk management programs, especially those that implemented enterprise risk management protocols, believes that risk management becomes a natural part of their continuous improvement culture.

I assume you are familiar with continuous improvement, which means that we are constantly working to improve what we are doing. This strive-for-quality attitude includes streamlining processes, rethinking work, reevaluating every goal, and eliminating unnecessary work and waste, all designed to make things better and lower the cost of doing business. This cultural norm must be included in an effective risk management program. If it is absent, your people will continue to take the same needless risks over again and again.

New or improved courses of action will arise from the cross-functional team approach of looking at risk. The chief risk officer (or focal point for your risk management program) is the person responsible for ensuring that each member of the risk management team commits to implementing the changes and improvements that have been identified and quantified.

Some organizations have turned this chief risk officer role over to the internal audit department, as we discussed previously. Whether it is considered to fit as a function of internal audit or a function of the risk management team, this group must constantly seek out improvement that could potentially lead to better risk evaluation techniques and more tools for employees to use. Additionally, this group must end weaknesses in strategies, identify metrics, establish goals, and instill rewards. In fact, the risk management team will end up monitoring your firm's culture mosaic.

It is essential to make sure your plan emphasizes and obtains firm commitments from employees who are responsible to be on the lookout for the conditions that lead to unnecessary or costly risk.

Action Plan: Tool for Planning for Risks

The tool that is best used for this step is the formalized action plan. An action plan is a visual definition or map of what it will take to make significant progress on a specific objective.

The payoff from using formalized action plans is their ability to communicate accountability to people. The contents of an action plan include the following:

- Overall strategic objective
- Deliverables and due dates
- Major steps
- Detailed steps
- Individual responsibilities
- Anticipated obstacles and challenges
- Performance metrics

Your action plan should define each level of change responsibility at the outset. Action plan participants include the following:

Sponsor. Person who has the ability to pay for the change and has ultimate accountability.

Advocate. Person who drives, wants, or demands the change.

Customer. Person who benefits from the change.

Agent of change. Person who carries the responsibility for facilitating the change.

Accountability partner. Person who will help to hold the change agent's feet to the fire; not quite a mentor, the change agent regularly reports back to this person about the progress (or lack of) made toward the plan's end state.

What the action plan tool is for:

- Highlighting overall objectives
- Showing expected or desired results
- Keeping track of actual results
- Holding employees to task
- Identifying risks in advance

Exhibit 10-1
Strategic Action Plan

A Strategic Action Plan or Initiative

Overall Strategic Goal: *Dispose of obsolete and dropped inventory products profitably.*
Measurable Strategic Plan Tactic: *Reduce inventory by 20 percent and improve the turnover from 4 turns to 6 turns.*

Connection to our risk management program:

In the company's risk management plan, we've addressed the concern that as a new company, we have not established sufficient protocols and controls to deal with obsolete inventories. We acknowledged in the risk management plan that we are in the negative cash flow position currently and will be for the next 18 months. Therefore, our inherent risk is that we may focus too much attention on managing cash, accounts receivable, and accounts payable and not enough attention on the balance sheet items unrelated to immediate cash flows.

Major Action Steps:

1. *Implement a plan to dispose of all aged inventory.*
2. *Implement a plan to dispose of all dropped products.*
3. *Establish controls to ensure the old and obsolete products are sold for their highest value.*
4. *Establish a way to provide an incentive for a sales employee to sell old products without hurting the sales of current products.*

Anticipated Obstacles and Challenges:

1. *Assigning the responsibilities to sell and ship the products to an already overworked staff.*
2. *Finding an inexpensive way to move inventory from the Ohio warehouse to the buyer.*
3. *Protecting Raelco's reputation, while disposing of obsolete products.*
4. *Convincing our suppliers to take back some products and issue credits.*
5. *Paying adequate incentive compensation to employees who sell the inventory, because there will be no profit margin to Raelco.*
6. *Determining the negative financial impact of the disposal and communicating this to the board and the bank.*
7. *Keeping the momentum needed to fully dispose of all obsolete products.*

Detailed Activities:

1. *Select the products for disposal (see SKU reduction plan).*
2. *Have the purchasing manager provide an analysis of the returnability of the dropped products.*
3. *Contact any companies who buy products like ours in bulk.*
4. *Hire a telemarketing person to handle the sale of smaller quantities.*
5. *Establish a commission or incentive plan for obsolete product sales.*
6. *Determine the approval levels for authorizing the sale price.*
7. *Prepare weekly updates and the status of sales and negotiations.*

Change Team:

Change Agents: Ron R., Keith J., and Donavon D.
Sponsor: Ron R.
Champion: Bob M. (executive)

Tool for Action Plan Reporting and Accountability

Exhibit 10-2
Action Plan Reporting Tool

Action Plans Summary

Employees Involved	Action Plan's Strategic Goal	Expected Financial Results: Increased Sales $$	Expected Financial Results: (Decreased) Expenses $$	Actual Results: Financial as of April 30, 2008	Actual Results: Non-Financial as of April 30, 2008
Sponsor—Ron R. Advocate—the Board Customers—Purchasing, Sales Agents—Ron, Keith, Donovan, Bob M.	Dispose of obsolete and dropped inventory products profitably	$5,000	$7,580		
Sponsor— Advocate— Customers— Agent—					
Sponsor— Advocate— Customers— Agent—					
Sponsor— Advocate— Customers— Agent—					

Definitions:

Sponsor— the person who has the ability to pay for the change.
Advocate— the person who wants or demands the change.
Customers— the recipients who benefit from the change.
Agents— the persons responsible for facilitating the change.

Exhibit 10-3
Personal Commitment Form

Tool for Obtaining Commitment

Activity: What is Your Next Step?

It is now your turn to do something to improve your own results. In the next few minutes, please complete the following:

1. Using the information I now have, I will use it for

2. Using the information I practiced, I will continue to become more comfortable by

3. Using the information we discussed, I will help my organization or coworkers by

4. I specifically need the following to be successful:

   Coach_____

   Mentor _____

   Specific training_____

   More support_____

5. I commit to taking these actions, and I will check back with myself to verify that I have done something on or around _____ (follow-up date).

   Date prepared_____

   My signature _____

   My accountability partner is _____

   I will check in with my accountability partner every _____ days.

Summary: The Importance of Step 5½

There is an old saying about the job not being complete until the paperwork is done. You can make the same case for your risk management plan. The plan is not executed until you see employees incorporate it into their daily behaviors. This is why this final (never completed) step is the bookend to step 1, where we define what risk is at a global level. Now to ensure that our risk plan works, we must move it down to risk at the individual level. This last step is accomplished by holding people accountable to what they commit to doing regarding the awareness, analysis, measurement, and management of risks undertaken.

11

Risk Management and the CPA

After completing this chapter, you should:

- recognize the impact that risk management is having on the CPA profession.
- add value to the discussion of risk for your clients or your employer.
- be able to use your understanding of the path of least resistance principle to isolate inherent and detection risk.

The Demand for Our Risk Awareness

As auditors and business advisors, we must recognize that our role includes providing assurance that controls are in place, and thus detect and monitor problems. Both the Committee of Sponsoring Organizations of the Treadway Commission's recent framework and Sarbanes-Oxley have created a new role for us: to become a key member of the firm's enterprise risk management team. Because a significant business risk could arise from nearly every decision and action undertaken by the firm's employees, we need to be very aware of the causes and contributors to costly risk. Sarbanes-Oxley has fostered both tremendous opportunities to serve our clients and great risks for those of us who report on financial statements as CFO or auditor.

> 34 percent of executives surveyed by Christian & Timbers felt that Sarbanes-Oxley should be repealed.
>
> Source: *Business Week*, May 23, 2005.

The Sarbanes-Oxley Act, the federal statute that added new rules for the governance of U.S. public firms, was the knee-jerk reaction that Congress put into action because of recent major ethical lapses. A major emphasis of Sarbanes-Oxley is on risk management. Therefore, for a firm to have a culture that aims for high integrity and strong ethics, its leaders must ensure that they weigh the cost of all major business risks, including the ethical ones, that they undertake.

What Sarbanes Oxley, the Securities and Exchange Commission, the accounting profession, and, yes, even Congress has been trying to get across to business executives since the 1970s is that there are big risks in running a business. The leader's clear responsibility is to identify each of the risks that could undermine the firm's goals and objectives and then address the risks before they blossom.

In the accounting profession, we place these risks into three categories:

- Inherent risk
- Control risk
- Detection risk

Most businesses do somewhere between a good to an adequate job of addressing their control risk. Internal controls, internal audits, and the like help leaders and boards of directors examine their checks and balances that need to be in place to hold people accountable.

Yet, breaches of ethics and rash decision making occur most often because CPA firms and their client's leaders fail to adequately address the first and third risks. Why? Because we also follow the path of least resistance and focus too much attention on control risk. That is what auditors have done since the beginning of time and still do.

Inherent Risk

Inherent risk is the susceptibility of a leader's assertion to a material omission or misstatement. The risk of such an omission or falsehood is greater for some assertions and types of transactions than for others. The primary cause of inherent risk may be both from internal and external sources. An example of inherent risk is the business model for developing commercial buildings that are built on spec. This means the builder must anticipate what the yet-to-be-identified purchaser might want in a commercial building. The inherent risks the developer faces in his business model are as follows:

- Tying up huge amounts of capital for long periods of time
- Mistiming the market for commercial property
- Dealing with regional economic conditions
- Changing trends in what commercial tenants want in their buildings
- Revising a nearly completed building to suit a new tenant

Control Risk

This is the risk that something material (quite large and significant) will be omitted or misstated and yet will not be prevented or detected timely. An example is where inventory in an offsite storage locker is not counted and no one notices. This means that the control designed to ensure that we count all inventory is at risk because it failed, and we did not detect the mistake.

Assertion

Whenever you state that something is true, you assert to its truth. In a company's financial statement, the CEO and CFO assert that the data and numbers in it are accurate to the best of their knowledge.

This is what the prosecutors tried to prove in the Enron and WorldCom cases: that the CEO was aware of the fraud, but asserted otherwise.

Detection Risk

Detection risk is the risk that the firm's employee, making an assertion, did not uncover or find a material omission or misstatement that exists in his statement about the accuracy or correctness. Detection risk is a function of both the effectiveness and application of an audit or testing process on the area at risk. The employee or auditor looking for detection risk can control it by carefully selecting and applying audit tests to the area. For example, at WorldCom, those who perpetrated the fraud of recording expenses as assets knew the external auditors only looked at capital asset transactions over $50,000. They made their entries under $49,999 to decrease the likelihood that the errors would be caught. For a long time, that strategy worked!

Risk management principle 10:

- Identifying risks in advance determines the likelihood that you will find the conditions that give rise to the risk.

This is why Sarbanes-Oxley requires that a firm conduct a risk assessment analysis within the context of the total operating environment.

Risk and Path of Least Resistance

Why do people naturally take the path of least resistance?

The path of least resistance is the principle that energy moves where it is easiest for it to go. It is the reality that a person will (almost always) take the course that is the most convenient or least painful.

The first thing an auditor and the CFO or controller must understand is the path of least resistance (POLR) principle. To do this, you need to study human behavior and be on constant vigilance for places that the POLR can exist. By discovering POLR for undesirable behaviors, you can easily shape behaviors to better ones. We can better understand the POLR with these truisms.

Risk management principles 11–13:

- When I display a behavior that increases risk, it is usually because my behavior is the path of least resistance. There is some sort of payoff for my actions.
- Temptations to take the path of least resistance come in many forms, most of which you are not aware.
- If I chose to shape your behavior, I need to alter the existing path of least resistance.

Answer these questions:

Why does the POLR principle show up in the workplace?

How does the POLR arise when there are no rules or guidelines for employees regarding risk taking?

How does the POLR arise when there are specific written rules or guidelines for employees regarding risk taking?

Where Auditors Need to Look

Client's Rewards

The actions and decisions that leaders reward tell employees what is most important. People pay attention to who is rewarded and why. If employees are rewarded for the wrong behaviors, other people see this and model those same behaviors. If a negative behavior is displayed by an employee and the action is either ignored or condoned, other employees see this and ignore the behavior or model it.

Very often, auditors will examine the formalized reward system of their clients, but they fail to investigate the informal rewards. This habit especially affects accounting departments because most accounting teams are in the business of catching other people's errors. We also see this as our sworn duty; we fix the error and rarely do something about the cause. In effect, when we do this, the accounting department and the firm's leaders have rewarded the behaviors that fostered the error in the first place.

Here are some questions to regularly ask of those whom you are auditing or supervising:

- Could someone who is in a position of power get away with a detrimental behavior?
- Why does this firm have or need rewards?
- What are employees being rewarded for?
- What form do they take?
- What sorts of messages do the formal rewards send?
- How are these positively aimed rewards being subverted?

Internal Pressures

Pressures to perform have the same impact on taking risks as rewards—and employees are almost always under some pressure to perform. In fact, the greater the need for the firm to take risks and the higher the rewards are for being innovative, the greater the likelihood for undue pressure placed on employees to achieve certain results exists.

There is a delicate balance between the incentive to achieve something and the pressure to perform. Applying pressure to achieve can be a positive tool that is often subverted. For example, the CEO may request that the sales group provide him with stretch numbers. If sales are higher than the original target, the sales team earns rewards or extra cash. This incentive crosses the line to the bad side when the pressure is so great, yet the employee lacks the tools or the means to achieve the higher target or is penalized for achieving the originally acceptable target.

There is a corollary to the POLR principle regarding incentives and rewards: if employees are shown a large carrot, yet cannot achieve it through legitimate means, and the carrot is something that they must have (to keep their job or pay the rent) the employee will almost always find a way to get the carrot. The means an employee uses may not always be justified. Remember, the ends must justify the means and not the reverse.

This corollary is often where unnecessary risk and unethical actions start: the pressure to perform combined with an incentive to perform combined with the inability to perform.

Here are some questions to ask yourself as you prepare to look for inherent risk:

- Do employees see a difference between a stretch goal and an unrealistic goal?
- Are employees required to explain the means to a predefined end?
- Are employees held accountable for how they achieve their goals, or just for achieving them?
- Where do pressures to perform or achieve a specific result come from, and why do they exist?
- How do employees normally respond to performance pressures?
- How do employees respond if the pressure is excessive or if the goal is unrealistic?

Ways to Alter Employee's Path of Least Resistance

- Limit the choices or options
- Eliminate all other possibilities so one choice remains
  The more choices employees have, the more likely that they will take the path that you may not approve of or recommend.
- Focus on the process instead of the result
  As described earlier, we have to hold people accountable for how they get the results as well as for achieving the results.
- Clarify and change the default choice

- Impose preconditions on each choice
  While we want employees to think for themselves, we also want to ensure that they think through each of their decisions before acting rashly or unwisely. Leaders need to model for their employees the default choice and explain to employees the real impact for each of the available options.
- Make the obvious choice the one with least pain or most pleasure
  Setting rewards for achievement is good and so is establishing penalties for lack of achievement. Whenever you use the carrot to induce good behavior, ensure that employees know there is a stick on the other end to encourage the good behavior.
- Make the choice by consensus
  The more people that are included in a decision, the more likely you will discover the risk and downside of each choice. Three heads are truly better than one.

Summary: Every Business Risk Leads to an Audit Risk

While Sarbanes-Oxley increased the awareness that risk management is important, business executives think that this is the accounting or the auditor's issue to face. This chapter serves as a wake up call. Unless the accounting profession can forcefully convince the owners and executives of our employers and clients that risk vigilance is really the way to do business and a cultural norm, we will continue to have more Enrons, WorldComs, and Freddie Macs in our future.

12

The Wide World of Risks

After completing this chapter, you should

- understand that risk comes in many forms and sources.
- be able to use this data to broaden your risk management plan.
- find many useful risk mitigation ideas.

Risk in Weather

Of course, everyone complains about the weather, and today the weather has become a major risk. Look at the results of the hurricanes in 2005 and the impact on Gulf Coast businesses and their employees. One strategy you can pursue to minimize the risk and cost of weather-related incidents is by taking a look at your insurance coverage. A recent article in *BusinessWeek* highlighted that some hedge funds are getting into this insurance business as a way of making money.

Risk in Geopolitics

Even violence from events that are unrelated to your business can spill over to your organization; therefore, we must have a response plan to address those should they occur. We saw this happen in downtown Seattle during the World Trade Organization demonstrations in December of 1999.

Due to globalization, leaders of organizations need to face up to political risk. You may not have bricks and mortar locations outside the United States, but your customer base, your distribution channel, or even your main suppliers could immediately be out of commission or subject to huge costs for doing business in some nations. The countries around the world have political leaders who feel that it is their right to change the rules in the middle of the game. Companies doing business in foreign markets also face up to the risk over confiscation or the appropriation of their property, politically motivated violence, and the problems of managing local currency.

As you can see, the ways that the company evaluates or perceives risk can have a huge impact on how it puts together its business model. Every company will continue to face new challenges they cannot predict adequately. But a comprehensive risk management plan with specific proactive methodology for identifying, assessing, quantifying, and mitigating risks increases your confidence in dealing with geopolitical issues that might involve your firm either directly or indirectly.

Risk from People Resources

Risk from Fraud and Employee Abuses

The overall loss from fraud is estimated to be over $660 billion or 6 percent of revenues. Fraud and abuse translates into $9 per day per employee.

How many employees work in your organization? _____

Multiply that number times $9 times 365. This figure will give you a compelling reason to be concerned about breaches in ethics in your organization!

White-collar fraud continues to grow. The 2004 *Report on Occupational Fraud and Abuse* from the Association of Certified Fraud Examiners (CFE) provided an estimate that the highest losses from white-collar fraud—46 percent—occur in businesses of fewer than 100 employees. These are the businesses that are less likely to have audits or have strong cultures of ethics.

Fraud is a crime based on concealment, and many organizations do not know that they are being victimized. Occupational fraud ranges from simple stealing of company assets to complex financial manipulation. Most frauds are either never detected or go on for years before they are discovered.

Small businesses are more vulnerable to breaches in ethics due to three factors:

1. They are less likely to require an audit.
2. They do not have a hotline for employees to report breaches.
3. They rarely have adequate internal controls.

One of the most common forms of fraud is kickbacks or conflicts of interest involving employees and others. Other forms of business fraud include the following:

- Fraudulent disbursements
- Skimming (cash stolen before the company has recorded it)
- Larceny (cash stolen after the company has recorded it)
- Fraudulent billings to fictitious companies or for fictitious goods or services
- Employees making false claims for compensation
- Employees requesting reimbursement for fictitious or inflated expenses

The CFE study estimates that 75 percent of all cash frauds come in the form of fraudulent disbursements.

Sarbanes-Oxley requires audit committees of publicly traded companies to establish procedures for "the confidential, anonymous submission by employees of the issuer for concerns regarding questionable accounting or other matters." Unfortunately, small businesses, which are not subject to Sarbanes-Oxley, fail to see the value or importance in this tool to detect fraud or abuse.

Hotlines will not always detect frauds, but they do create a reporting mechanism for employees that allows for the collection of tips on possible wrongdoing. Firms that use such a hotline are more likely to be aware of potential frauds with employees but also with customers, vendors, and third parties. Firms that utilize employee hotlines or some sort of anonymous and safe reporting mechanism show the greatest decrease in actual frauds. A key element in almost every discovered fraud is a dishonest employee who had the opportunity to commit the infraction.

What I find most interesting is that the CFE survey found that over half the frauds committed by an owner or executive were detected through an anonymous tip!

More CFE findings were that

- only 6 percent of the frauds were caught via the firm's internal controls.
- 33 percent of frauds in small business involve a billing scheme.

- 33 percent of frauds involved check alteration.
- 82 percent of fraud cases were asset theft.

Finally, the CFE study concluded that for the small businesses included in the study, only 31 percent had any form of internal audit or fraud examination department.

Those surveyed in the study gave their opinions about today's business environment:

- 67 percent say that fraud is worse today than five years ago.
- 70 percent say fraud detection is getting better.
- 75 percent say fraud detection resources are not adequate.

The CFE's 2004 study's results are consistent with those of their 2002 study.

Warning Signs of Situations at Risk for Unethical Behaviors

The following make up the 80 percent of people who would defraud you if they could and the 10 percent that will anyway.

- Employees who are being downsized
- Employees who are bored and looking for excitement
- Employees who find a hole in the company's internal controls, benefit from it, and do not report the lapse
- Employees who enjoy bending the rules
- Employees who are under personal stress
- Employees who experience personal financial problems or setbacks
- Employees with addictions, such as alcohol or gambling
- Employees who need to be the center of attention

Risk in Your Static Rewards

Behavior never remains static. As a leader you must be willing to alter your visible and invisible reward systems, your compensation systems, your people systems, and your communication systems whenever employees show behaviors that lower the ethics of your organization.

Change your compensation system and employees will automatically change their behavior. The job of the twenty-first century leader is to drive desired behavior and model the high standards of the organization.

Risk in Employment Compliance

Another area to address in your risk management plan is compliance with worker health and safety regulations. As with all regulations, it is difficult for companies to keep up, yet expensive if they are unable to comply with the latest changes.

Lawsuits, including those for wrongful termination, product liability, discrimination, and sexual harassment have mushroomed in the last decade for many reasons, including the Civil Rights Act of 1991. This increase requires every leader in our organization to adopt a diligent awareness of where risks can occur in relationships between employees and their employer. You must be able to use every tool available to you. Related to this risk is workplace violence, which continues to grow as a threat from upset employees. Business leaders continue to use downsizing or rightsizing, but this competitive tool has a huge negative impact on the employees who lose their jobs and livelihoods. Terminations often turn into a situation where

disgruntled employees exact revenge. Many previous cases of such outbursts were triggered by mergers or downsizing. Your company needs to pay very close attention to your people problems of all magnitude and to employees' emotional states, which arise from these difficult situations.

It's Real!

I lead annually a workshop based on a colleague's materials and research. This course on human resources compliance is for CPAs and human resources managers of small to medium organizations. Each time I present it I find that every organization respresented is breaking the law in numerous ways on compliance. This finding also applies to the CPA firms who are providing their clients bad and erroneous, and often illegal, advice.

Risk in the Technology Dependent Age

Risk in Information Security

In today's world, we all rely heavily on our computers and a wide range of technology. This progress puts all of our firms in an extremely vulnerable position because we are only as good or as secure as our information security systems. The following are some examples of where today's dangers or risks in information security occur:

- Airborne assaults from electronics such as a smart phone or a personal digital assistant (currently, the hacker's choice is Blue Tooth)
- Anti-Web sites set up to defame your company
- Attacks in networks linking home and business computers
- Children's access to technology
- Corporate spies
- Cyber smearing
- Cyber terrorists
- Disgruntled employees
- Electrical blackouts (local, regional, or national scale)
- Foreign intelligence
- Frauds, such as phishing
- Hackers and crackers
- Hidden cameras in bathrooms and changing rooms placed there by employers or others
- Organized crime groups
- Legitimate Web sites hijacked for pornography purposes
- System cracking through server computers where legitimate Web sites are housed
- Spyware
- Targeted mass mailings of worms and viruses or Trojan horses
- URL squatters who look for prominent sites where the owners have not renewed the registration
- WiFi systems and wireless networks

In 2006, an estimated $350 million alone was spent to deal with Spyware.

Answer this question:

How many have you included in your firm's risk management strategy or risk portfolio?

Information that is leaked outside the organization can have an impact on the company's fortunes plans, reputation, and marketing efforts. Inadequate patent protection of your inventions can cost you your competitive edge and potential profits. As a leader, you must be proactive in protecting every single piece of sensitive information from loss or theft. We want this protection 100 percent of the time, but that would be impossible and incredibly expensive. For example, a typical office desk is a virtual gold mine of sensitive information. One outsider rifling through your employees' desks could find tremendous information that could be valuable to someone outside of your organization.

It is imperative that you, the leader, ensure that every employee understands the nature of sensitive information and incorporate proactive protection and security training into your everyday basic security techniques. Likewise, when an employee who is knowledgeable leaves your organization, you must do every thing to secure both the company information and sensitive data.

E-Commerce Risk

The best approach to addressing risk management today is a proactive stance anticipating your risks and working to keep them from biting your firm. This will help you to prepare for today's fast-paced and global world of business. A thoughtful and proactive strategy prevents or anticipates problems in the first place, creating the need for a formalized risk management program. An effective risk management plan can help you deal with bad publicity, help reduce insurance costs, and keep your business running smoothly in the face of Murphy's Law.

E-commerce is changing the business world beyond just an opportunity to generate more revenues. E-commerce affects privacy, security, and intellectual property. The business risks of e-commerce go beyond hackers and network breakdowns because they threaten the very existence of your business and entire market segments. As part of your risk management strategy, you need to assess whether your products could become redundant or obsolete and how your existing sales or delivery methods may be affected by e-commerce.

Risk of Sabotage

We refer to them as "hackers" or "crackers" or worse, but there is a difference. Hackers are in your system for a joyride. Crackers are there for a malicious purpose. They want to steal some information, store stuff on your server, slip you a virus, access your cash, or make you look stupid in public. Crackers in your system could leave you liable for their handiwork. Some examples:

- Your bank might expect you to pay for credit card losses should a cracker dig into that system.
- Vendors would expect repayment for the stuff that the cracker ordered through your systems.
- Employees, of course, could sue because you failed to keep their files confidential.
- Partners could claim damages for intellectual property being disclosed to the wrong parties.
- Shareholders could sue you for losses to their investment.
- Governmental regulators could treat you as incompetent for your ineptitude.

Worst of all, your insurance company may decide you were negligent in protecting yourself against crackers and decline to reimburse you for your defensive costs. It can be expensive not to have a risk management program, especially one designed to look at the risks in the applications and misuse in your technology.

Hackers and crackers have penetrated such organizations as NASA, Los Alamos, the Pentagon, the IRS, the White House, the FBI, and AT&T. No one is exempt from where they decide to go.

The odds of any external invasion into your technology systems are smaller than the odds of someone within your organization accessing and exploiting your resources. Far more likely risks include the following:

- A disgruntled employee
- A cleaning crewmember who rifles through someone's desk
- A bookkeeper who creates a false vendor
- A supplier who is in collusion with your product manager
- An employee who is pulling racist or sexist jokes from the Web and passing them on
- A customer who is using you to extract the best terms available

A crime or fraud instigated from the inside or outside will be committed with computers. In every organization and in every industry, it is inevitable.

Small businesses can take some comfort in this: the greater the potential loss, the greater the chance of crime. This means that a cracker may have more opportunity to benefit from invading AT&T than from invading the neighborhood daycare. This does not mean, however, that you are free from being concerned about these sorts of risks. An invasion or misuse of your firm's computer system can lead to financial devastation. This places risk squarely in the lap of the executive team. Hackers and crackers are persistent and as adaptive as cockroaches and will always be trying to get into your organization.

Sabotage Mitigation

Your solution is to develop an overall strategy and make the decision to mount a cost-effective defense. You must establish a strict prevention policy, then manage and minimize the risk through whatever steps necessary to prevent financial loss or disaster for the misapplication of the company's information systems. This means that all technology risks must be recognized, prioritized, and their impact minimized in your risk management plan.

Today, information stored in our files and databases is often the company's most valuable asset, yet it is given very little attention from a security standpoint. Our firm's leaders must prioritize our information assets according to their worth to the business model and to business continuity. They need to pay attention to protecting the information that is most valuable. A loss could be the disappearance of information caused by a virus, or it could also be the transference of information into the wrong hands. Sadly, such transfers of information in some states do not qualify as thefts. Just as bad as a loss of your data is the serious loss of face to customers, the public, and your shareholders. No executive that I know of wants their picture and name identified on page one of the *Wall Street Journal* telling how their system was broken into by a cracker.

A key part of your risk management program is a disaster recovery plan that includes recovery of data and dealing with the possibility of secure information going outside of your normal channels.

Sabotage and vandalism are alive and well and more costly than the theft of information. A total system security model needs to touch every aspect of the organization, looking for potential threats and identifying the risks factor, including the cost to recover. An example of how this risk escalates is the cost to recover a patent. If one of your patents gets into the hands of a competitor, you have the right to sue and protect your right, though the suit may cost more than the original investment in the patent. Of course there is no guarantee that you could collect even if you win.

Some technology experts believe that almost all acts of information theft and cyber sabotage are considered inside jobs. That does not mean that the hacker or cracker is a former employee. It does imply that one or more of your employees was lax in the security system that allowed the outsider into your system.

This laxness can include the following:

- Not regularly changing passwords
- Using easy-to-identify passwords
- Passwords written down in Rolodexes
- Passwords posted on the walls of an employee's cubicle
- Passwords written on sticky notes posted on the computer screen

The ingenuity of today's cyber crook will challenge your best efforts and intentions. The only effective corporate policy is not one in your procedure manual, but rather an attitude of constant diligence and consistent improvement and a thoughtful and consistent risk management plan.

Risk to Personal Data

A recent *Wall Street Journal* and NBC poll identified privacy as American's number one concern. The U.S. Governmental Accountability Office (U.S. GAO) reports a five-fold increase in allegations of Social Security number fraud in the survey period from 1998 to 2001.

People's personal information is not only stored in your firm's computers, it is also contained in your old file cabinets, discarded boxes, and, of course, the landfill. No controls over this data will ever be 100 percent secure, and every one of us is at risk, especially if your employees use such information in ways that violate your policies. One of the ways that you can protect yourself is to safeguard both your incoming and outgoing mail. Another way is to shred all business documents by a professional and bonded shredding company.

Risk in E-Mail

The risk of someone mistaking your e-mail communication for spam grows each day. It is estimated that the average person spends between two and two and a half hours a day sorting e-mails with anywhere between 50 percent to 75 percent of those e-mails considered spam or junk.

- 80 percent of e-mail users are bothered by deceptive or dishonest content.
- 62 percent of companies use filters to block spam from employees' e-mail accounts.
- 25 percent of e-mail users say that the ever-increasing volume of spam has increased their overall time spent dealing with e-mail.

Spam-related regulations both in the United States and Europe have defined what organizations can and cannot do with spam. This does not mean that unscrupulous spammers will follow these rules. To help protect your organization's risk, it is good to not only be aware of these regulations, but follow them. The scope of the regulations that we all face in both the United States and Europe cover even a single e-mail that you send to a business, partner, or a customer.

Recently, the AICPA, in combination with the Canadian Institute of Chartered Accountants has issued a privacy framework that members and nonmembers can use to help ensure our legitimate e-mail is not classified as spam and possibly subject your organization to a lawsuit as a spammer.

Risk in Internet Privacy

Privacy on the Internet is a big concern. Consumers are becoming increasingly angry when their personal information is used without their permission. Some regulations have been and will continue to be introduced in order to prevent companies from releasing sensitive customer information to third parties

without the consumer's express consent. Consumers are fearful that businesses like yours and its Web sites are not adequately protected from either an outside invasion or predatory practices by your organization.

U.S. Regulations on Web Site Risk

In the United States, the protection of an individual's information is governed by laws, court rulings, and self-regulation. Alternatively, certifying organizations (like the AICPA or Congress) rely on the members self compliance. Here in the United States, the four Fair Information Practices of user security on a Web site are as follows:

Notice. Give users notice when you are collecting their information and tell them how it will be used and to whom it is disclosed.

Choice. Give users the option of opting out of giving personal information and the option to approve of sharing their information with third parties.

Access. Give the user reasonable access to the information you have on them and give them the ability to correct all erroneous data.

Security. Establish reasonable measures to protect users' data.

In 2000, the Federal Trade Commission (FTC) found that only 20 percent of the most visited Web sites they surveyed had implemented all four of the Fair Information Practices. Of the most popular Web sites, 42 percent had implemented, at least in part, one of these four cornerstones. The FTC also found that only 8 percent of the sites in a random sample displayed any type of privacy seal.

European Regulations on Web Site Risk

Passed in 1995, the E.U. Privacy Directive has important implications for both companies engaged in e-commerce and for multinational corporations with offices in European countries. The directive is based on the idea that collecting and using personal information infringes upon the fundamental right to privacy and covers a wide variety of data that might be transmitted during the normal course of business. Businesses that want to trade in E.U. countries must guarantee that the user's personal data is

- processed fairly and lawfully.
- collected for specified, legitimate purposes.
- accurate and up-to-date.
- kept only for the stated purposes and nothing more.

In addition to the U.S. minimum standards of notice, choice, access, and security, the E.U. directive requires three more user protections:

Onward transfer. You can only disclose user information consistent with your published notice and choice standards.

Data integrity. You must take reasonable steps to ensure that all user data collected is accurate, complete, and current.

Enforcement. You must place mechanisms to give users recourse if a complaint or a dispute arises.

The term *user* in both the U.S. and E.U. standards refers to individuals, but it would add to your reputation for integrity if your firm applies them to the businesses that visit and use your Web site.

The bottom line is that all businesses must take consumer privacy issues seriously. This will require you to invest resources to secure both your internal databases and your Web site. Your firm's leadership must also determine if your insurance covers lawsuits that may arise over privacy issues. All organizations with an online presence will need to establish online privacy statements certifying that they comply with the current privacy standards both here and abroad. Make sure your Web site and Internet presence is covered in your risk management plan.

Risk of Internet Rumors

The Internet has accelerated the way that the stock market reacts to information both good and bad about companies. A new phenomenon that has grown is called cyber smear. The reasons for cyber smear are sometimes economic profit and personal gain, but they are not exclusively the reason more and more firms and their owners are finding that the Internet can facilitate low cost cyber smear campaigns. In a number of cases, the cyber smear campaign was motivated by revenge. Messages are posted by disgruntled employees or insiders, ex-employees, envious ex-colleagues, competitors, creditors, and even people seeking a forum when they are denied employment with you.

Ways that companies can protect themselves are to monitor the stock chat message boards at Yahoo Finance, Raging Bull, and Silicone Investors. Other companies are protecting themselves against this risk by hiring third parties that specialize in a service of checking the Internet for cases of potential cyber smear. This protection is expensive but may be worth it the more likely a target you are. A good place to start is by visiting the eWatch Web site (www.Ewatch.com).

A few years ago when I was doing a project with Costco, they experienced how seriously an Internet rumor can quickly affect the stock market. Their CFO, Richard Galanti, had informed analysts that the next quarter's profits would be between (not the real numbers) $0.25 and $0.30 a share. As the reporting day grew closer, someone started a rumor via the Internet that Costco would not meet its profit targets. The day before Mr. Galanti's scheduled call to the analysts, Costco's share price dropped 20 percent because of the rumor. In reality, Costco met the stated profit target, but the damage had already occurred. Employees, most of whom are shareholders, were spooked about the sudden drop. Costco's president and CEO Jim Sinegal had to spend considerable time over several days calming numerous employees' fears and explaining that the reaction was based on a falsehood that had been accepted as fact.

Summary: The Importance of These Risks

Do you ever wish to go back to a day when life was simpler? I would bet that we have all entertained such a harmless desire. What is harmful is if you were to attempt to live your life as if life contained no complexity at all. In fact, that could be dangerous. That is why we need to pay attention to the many types of risks contained in this chapter. The likelihood of your firm being subject to all of them is remote. However, if your business is growing and becoming more innovative, people in your organization will open Pandora's box to risk.

In an effective risk management plan, as you have discovered, it is important that leaders look globally at all the potential risks that could undermine the firm's success. The more information you have available to you, the more risk savvy you will be. Therefore, knowing that all these possible risks are out there, from organized crime groups to cyber smears and Internet rumors, helps everyone in the organization to be both wary and aware. These two attitudes, in combination, help employees and leaders become better risk managers.

Appendix A

Tool for Culture Risk Assessment

An amazing tool was developed by Robert Simons, a professor of business administration and director of research at Harvard Business School. Simons' tool, which he calls the risk exposure calculator, helps managers and leaders to determine the amount of internal risk to which they expose their businesses. The calculator consists of three pressure points. They are as follows:

Pressure Point No. 1: The Growth Factor

Fast growing businesses are intense and exciting, but also create pressures to perform. Fast growth leads us to promoting or hiring inexperienced personnel into key positions. Each one of these pressure points, if handled correctly, leads to greater success. However, if handled poorly, it fosters greater risk exposure.

Pressure Point No. 2: The Corporate Culture

The internal workings of the organization, known as its culture, significantly affect people's approach in viewing risk. Simons identified three specific areas within this pressure point:

- Rewards for entrepreneurial risk taking
- Executive resistance to bad news
- The level of internal competitiveness

Pressure Point No. 3: The Management of Information

A fast-growing organization must have the ability to obtain timely and accurate feedback. Without this ability, bad news is often late, mislaid or, even worse, transformed into good news. The three concerns of this pressure point are as follows:

- Transaction complexity and velocity
- Gaps in diagnostic performance metrics
- The degree of decentralized decision making

Then, based on how the decision makers view their own organization, Simons' calculator becomes self-rating. Organizations with low scores are in the *safety zone*. Companies with medium scores are in the

caution zone. Firms with the highest scores are in the *danger zone*. Simons' tested his risk exposure calculator on hundreds of different companies that attended Harvard Business school's executive education programs.

Simons' tool then asks five questions that help managers understand the relationship between risk and reward. He helps managers to see that they have four levers that they can use to control risk as their company pursues its specific strategy. The four areas he identified as levers are as follows:

1 The firm's belief systems
2. The firm's boundary systems
3. The firm's diagnostic control systems
4. The firm's interactive control systems

Working together, these four levers give managers and executives the tools to balance profits and growth with control. Each of these levers must be carefully aligned with the firm's global strategy.

Simons next asks executives to answer these five questions. As a whole, the answers create awareness about their firm's control environment over risk management:

- Question 1—*Have your senior managers communicated the core values of the business in a way that people understand and embrace?*
- Question 2—*Have your leaders clearly identified the specific actions and behaviors that are off limit?*
- Question 3—*Are your diagnostic control systems adequate at monitoring critical performance variables?*
- Question 4—*Are your control systems interactive and designed to stimulate learning?*
- Question 5—*Are you paying enough for traditional internal controls?*

The full force of question 5 forces the executive to see how the leaders value the control systems overall, because, as a company grows, the money invested in the control systems must grow commensurately.

Appendix B

Ethics Focus: Business and Industry

Ethics Overview

Compliance with ethical and professional standards is at the very heart of what it means to be a CPA. Our profession was founded on the qualities of honesty, trustworthiness, being free of conflicts, doing what is right, and having due and proper support for our work and opinions. The need for all of us to uphold these values is just as true today as it was more than 100 years ago, when CPAs first became a key part of the financial reporting process. Ethical compliance is, however, not just a luxury afforded to us. In the current environment of expanded responsibilities and transparency, greater liability, and new civil and criminal penalties for failure to meet professional standards, each of us is personally and professionally obligated to know and understand our ethical duties. The AICPA and state societies are committed to increasing awareness of ethical issues among our membership and assisting professionals in implementing and sustaining the high ideals of our profession.

Studies have shown that management's demonstrated commitment to ethical behavior means far more to employees than codes of conduct and training programs. How do you demonstrate this commitment? By "setting the proper tone at the top," fostering the development of an ethical corporate culture, and reinforcing positive organizational values. This means you and your company's senior executives need to take part in implementing ethical standards, enforcing these standards, and providing positive feedback in response to actions that support an ethical environment. Whether you are the CFO or an entry level staff accountant, keep in mind that your actions both form a part of your business's value set, and reflect on you and others in the organization.

Recent Developments

In 2006 and early 2007, the persistent drumbeat of media reports concerning wrongdoing at public companies stressed the continuing need for vigilance in accounting, financial reporting, compliance and governance activities. Although financial restatements were expected to decline substantially in the years following larger public companies' implementing internal control assessments and obtaining internal control over financial reporting (ICFR) audits under Section 404 of Sarbanes-Oxley, that expectation is being swamped by the tide of restatements now underway. Published statistics indicated that 2006 was another record-setting year for restatements, with (*a*) public companies having less than $75 million in market cap witnessing a 40 percent increase in restatements from 2005 to 2006, (*b*) public companies with a market cap of $75 million or more that have been required to comply with Sarbanes-Oxley Section 404's ICFR audit provisions experiencing only a 14 percent decline in restatements from 2005 to 2006, and (*c*) an increase of 30 percent in "quarter only" restatements in 2006 having contributed to the overall rise in restatements among public companies.

Against this backdrop, the options backdating scandal continued to mushroom through the filing of civil and criminal charges against various CEOs, CFOs and general counsels to public companies accused of knowingly backdating options granted to themselves and other employees. Greg Reyes, the former CEO of Brocade Communications, was convicted in August 2007 on 10 felony counts of securities fraud for backdating options provided to employees between 2000 and 2004. BDO Seidman LLP was found guilty of gross negligence in connection with the financial fraud at E.S. Bankest LLC, which resulted in the loss of $170 million in investor funds when the financial services company filed for bankruptcy.

Small audit firms and their clients also were not immune from allegations of financial fraud or obstruction of justice. For instance, the engagement partner at the auditor for the Roslyn School District was indicted on 26 counts of tampering or falsifying business records, tampering with physical evidence, and offering a false instrument for filing after the New York State Comptroller's office and the Nassau County District Attorney's Office began audits and investigations into the finances of the Roslyn School District. After pleading guilty to tampering with public records, the audit partner on the Roslyn School District audit was sentenced in 2006 to four months in jail and five years of probation for his role in altering school district records that were submitted to the New York State Comptroller's office and the Nassau County District Attorney in connection with their audit and investigation. At least four Roslyn School District officials pled guilty or were convicted on various charges including first- and second-degree larceny in connection with their embezzlement of school district funds.

What do these developments say to CPAs in industry, and what issues do CPAs need to consider in light of these developments?

- Deep-seated moral and ethical problems that manifest themselves through fraudulent financial reporting haven't disappeared since the heydays of Enron, WorldCom, Tyco, Xerox, Computer Associates, Adelphia, and other companies.
- Internal audit functions need to use a risk-based, forward-looking approach to evaluate areas of exposure for deficient financial reporting—reconsider often Statement on Auditing Standards No. 99, *Consideration of Fraud in a Financial Statement Audit* (AICPA, *Professional Standards*, vol. 1), factors when preparing or implementing an internal audit plan.
- While revenue recognition is a perennial financial reporting issue, others of recent significance include fair value measurements, accounting for quasi-debt, equity instruments and beneficial conversion features, accounting for reorganizations and restructurings, defined benefit pension and other retirement plan accounting, stock and option compensation expense, and quantifying financial statement misstatements through considering quantitative and qualitative factors and the impact on the balance sheet and income statement.
- Executive compensation issues, highlighted by the options backdating scandal and enhanced disclosure requirements, which came into effect in 2007, will continue to draw media, investor and regulatory scrutiny.

CPAs employed in industry must be mindful of part 1 of paragraph .02 of ET section 91, *Applicability* (AICPA, *Professional Standards*, vol. 2): "The Rules of Conduct that follow apply to all professional services performed..." and the provisions of the AICPA's bylaws that require members to "adhere to the Rules of the Code of Professional Conduct." Taken together, these provisions make clear the obligations of members to adhere to the Code of Professional Conduct, regardless of whether the member is engaged in public practice or is employed in industry.

Key Ethical Dilemmas

CPAs in industry face special and unique challenges in fulfilling their ethical responsibilities, particularly because they are accountable to multiple constituencies. Caught between the board of directors, audit committee, outside auditors, internal audit personnel, stockholders, and regulators, industry CPAs can find themselves being pulled in countless directions. Because more than 80 percent of fraudulent financial reporting has historically originated with the CEO or CFO of a business, pressures on industry CPAs from higher-ups in the organization can create intolerable situations or even force life-changing decisions. When faced with these circumstances, you need to make the right choice—not the easiest choice or the most expedient. Let us review a few of the more common ethical dilemmas that you may run into as an industry-employed CPA.

Integrity and Objectivity

- If I am uncomfortable with disclosure or an entry in the financials, but I have been overruled by my superior, what should I do? Do I have to do anything?
- To what extent am I responsible for preparing our financials in accordance with generally accepted accounting principles?
- I've heard that when prosecuting employees involved in financial frauds, the government has dealt more harshly with CPAs accused of wrongdoing. Why is that? What does this fact mean to me?

Reporting and Disclosure Protocols

- How far can materiality be taken when applying judgments to financial reporting? What policies and procedures should I apply to enhance the quality of our reporting?
- If my company uses the rollover approach in analyzing financial statement misstatements, what is my obligation when considering materiality issues?
- I have become aware of an internal control deficiency—now what?
- Our company engaged a private investigator that is using subterfuge to gain access to phone records of customers and suppliers, and I've become aware of this—what are my professional responsibilities to my employer? What should I do now?
- What are the professional standards that apply to us when making estimates and judgments? What disclosure protocols need to be followed when discussing estimates?

Independence and Due Care

- As an employee, I am not independent—am I still bound by independence concepts?
- As an industry CPA, what is my supervisory responsibility for others?
- I supervise the tax function at our company. Do I have any special obligations in that position?

Confidentiality

- When does my duty to be candid with the outside auditor override my duty of confidentiality to my employer?

Nonattest Services and Relations with External Auditors

- What approvals must we get for nonattest services from our audit firm? From whom?
- Can we hire someone from our outside audit firm without impairing its independence?

- Our company is interested in getting advice on an aggressive tax shelter that's been proposed to us by a third party. Can we discuss the shelter with out audit firm?
- Our audit firm has always helped us out by preparing the CFO, controller, and assistant controller's personal tax returns. Can they still do this without impairing independence?

Addressing Ethical Dilemmas

When you encounter an ethical dilemma in management services, bear in mind the following professional conduct principles, among the most important in our profession. You can access the complete AICPA Code of Professional Conduct at www.aicpa.org/about/code/index.html.

- Be "guided by the precept that when members fulfill their responsibility to the public, clients' and employers' interests are best served." (ET section 53, *Article II—The Public Interest* [AICPA, *Professional Standards*, vol. 2, par. .02])
- Test decisions and deeds by asking, "Am I doing what a person of integrity would do? Have I retained my integrity?" (ET section 54, Article III—Integrity [AICPA, *Professional Standards*, vol. 2, par. .03])
- "Although members not in public practice cannot maintain the appearance of independence, they nevertheless have the responsibility to maintain objectivity in rendering professional services." (ET section 55, *Article IV—Objectivity and Independence* [AICPA, *Professional Standards*, vol. 2, par. .04])
- "Members employed by others to prepare financial statements or to perform auditing, tax, or consulting services are charged with the same responsibility for objectivity as members in public practice..." (ET section 55 paragraph .04])

Available Resources

Accounting professionals have a multitude of resources available to provide guidance on ethical issues. In addition to the Code of Professional Conduct and the Interpretations and Ethics Rulings under the Code, each state has its own code that has been adopted by the state society or state accountancy board. Many states maintain ethics hotlines staffed by knowledgeable CPAs who are trained to give you advice on how to handle specific ethical issues. Further guidance is available from rules adopted by the Securities and Exchange Commission, the Public Company Accounting Oversight Board, the Governmental Accountability Office, the Federal Deposit Insurance Corporation, the Department of Labor, and other government regulatory agencies.

The AICPA offers several continuing professional education (CPE) courses designed to explore common ethical issues encountered by accounting professionals, among which are *Real Word Business Ethics for CPAs in Business and Industry: How Will You React, Real World Business Ethics for Tax Practitioners: How Will You React, and Real World Business Ethics: How Will You React?* These programs feature true-to-life cases involving topical ethical issues—set in the context of tax, management reporting, audits, forensic investigations, and consulting and advisory services. If you are looking for an up-to-date ethics refresher in an interactive, case-based setting, we encourage you to contact your state society to find out when they will be offering one or more of these courses. You can also access individual case studies from these courses through CPExpress. Each individual case study carries one hour of CPE ethics credit and asks you to address an ethical dilemma you may face in various positions such as CFO, corporate controller, forensic investigator, audit engagement partner, engagement quality review partner, tax return preparer, amended return preparer, or merger and acquisition consultant.

The AICPA also has a broad range of ethics information available for members at www.aicpa.org/Professional+Resources/Professional+Ethics+Code+of+Professional+Conduct/Professional+Ethics/Resources+and+Tools/, including frequently asked questions, alerts and guidance, ethics exam materials, and current developments in ethics, such as rule updates, exposure drafts, and comment letters. You can also

hyperlink or go directly to CPExpress at www.cpa2biz.com, where you can take online or self study CPE courses on independence, professional ethics, and other selected ethics topics. If you need ethics assistance, you may also contact the AICPA Ethics Hotline by calling (888) 777-7077 (press menu option 5 and then option 2) or e-mailing ethics@aicpa.org. You can visit the Professional Ethics Division's Web page to review changes to independence and other standards, as well as implementation guidelines for these standards, adopted under the Sarbanes-Oxley Act of 2002. You can also review ethics articles published in the *Journal of Accountancy, The CPA Letter*, and *The Tax Adviser* through the AICPA Web site.

The Professional Ethics Division's Web page also has a link to *Ethics Information for CPAs in Business & Industry* that has resources specifically meant to assist members who encounter work-related ethical dilemmas or questions. Under this link, you can review general ethics questions, a sample ethics case, specific questions and Code answers for ethical questions pertaining to those in business and industry, and ethics quizzes designed to test your knowledge. In addition, you can download an ethics decision tree developed by the AICPA and the Business & Industry Executive Committee to assist members in exploring and analyzing ethical issues that can arise in work-related situations.

Glossary of Controllership and Financial Management Terms

absorption costing. A costing method that treats all manufacturing costs (direct materials, direct labor, variable overhead, and fixed overhead) as product costs. It is also referred to as full costing.

accept or reject decision. Decision resulting from a relevant cost analysis concerning whether to accept or reject a special order.

accounts payable turnover ratio. A liquidity measure that shows the number of times on average that accounts payable are paid during the period; calculated by dividing net credit purchases by average accounts payable during the period.

accounts receivable turnover ratio. A liquidity measure that shows the number of times on average that accounts receivable are collected during the period; calculated by dividing net credit sales by average accounts receivable during the period.

action analysis report. A report detailing the costs that have been assigned to a cost object, such as a product or a customer; it also shows how difficult it would be to adjust the cost if there were a change in activity.

activity. An event that causes the consumption of overhead resources within an organization.

activity cost pool. A "bucket" in which costs that relate to a single activity measure are accumulated within an activity-based costing system.

activity measure. An allocation basis within an activity-based costing system which, under ideal conditions, measures the amount of activity that drives the costs in an activity cost pool.

activity-based costing (ABC). A costing method that focuses on individual activities as primary cost objects and uses the costs of these activities as the basis for assigning costs to other cost objects, such as products and services.

activity-based management (ABM). A management approach that focuses on managing activities as a way of eliminating waste, reducing delays, and minimizing defects.

administrative cost. Any executive, organizational, and clerical cost associated with the general management of an organization.

amortization. The process of allocating the cost of an intangible asset over its estimated useful life.

asset turnover rate. The sales divided by the average operating assets figure. It represents the amount of sales generated from each dollar invested in operating assets by an investment center.

average age of inventory. The number of days on average that a company holds inventory before it is sold; calculated by dividing 365 days by the inventory turnover ratio.

average collection period. The number of days on average that an account receivable remains outstanding; calculated by dividing 365 days by the accounts receivable turnover ratio.

average payment period. The number of days on average that an account payable remains unpaid; calculated by dividing 365 days by the accounts payable turnover ratio.

balanced scorecard. An integrated set of financial, customer, internal business processes, and learning and growth performance measures that is derived from and supports an organization's strategy.

benchmarking. A study of organizations considered to be among the best in performing a particular task. Involves establishment, through data gathering, of targets and comparators, through whose use relative levels of performance can be identified.

bottleneck. Any machine or other part of a process that limits the total output of an entire system.

break-even point. The level of sales, in units or dollars, where profit is zero. It can also be defined as the point where total sales equals total fixed and variable costs, or the point where total contribution margin equals total fixed costs.

budget. A detailed plan for the future acquisition and use of financial and other resources over a specified period of time, usually expressed in formal quantitative terms.

business process. The series of steps followed when carrying out some task in a business.

capital budgeting. The process of planning significant outlays on projects that have long-term implications, such as the acquisition of new property and equipment or the introduction of a new product line.

capital lease. A long-term agreement that allows one party (the lessee) to use the asset of another party (the lessor) in an arrangement accounted for like a purchase.

cash budget. A detailed plan showing the primary sources and uses of cash resources over a specific time period.

cash debt coverage ratio. A measure of solvency that can be calculated by dividing cash provided by operating activities by average total assets.

change management. The process of coordinating a structured period of transition from one situation to another in order to achieve lasting change within an organization. It can be of varying scope, from continuous improvement to radical and substantial change involving organizational strategy.

chief financial officer (CFO). Top management team member responsible for providing timely and relevant data to support planning and control activities and for preparing financial statements for external users.

committed fixed cost. Any fixed cost that is considered to be difficult to adjust because it relates to the investment in facilities, equipment, or the basic organizational structure of a firm

common cost. Costs that are incurred to support a number of costing objects but that cannot be traced to any one of those costing objects individually.

constraint. Any limitation under which an organization must operate, such as limited available raw materials or machine time, that restricts the organization's ability to satisfy demand.

contribution margin. The difference between total sales and total variable cost, or the difference between unit selling price and unit variable cost. It represents the amount contributed to covering fixed costs and providing a profit to the organization.

contribution margin ratio. The ratio of total contribution margin to total sales, or the ratio of unit contribution margin to unit selling price. It is used in cost-volume-profit analysis.

control. The process of establishing procedures and then obtaining feedback in order to ensure that all parts of the organization are functioning effectively and moving toward overall company goals.

controller. The manager in charge of the organization's accounting department.

controlling. Ensuring that a plan is actually implemented and appropriately modified as circumstances change.

conversion cost. Costs of converting raw materials into finished goods. It is the sum of direct labor costs plus manufacturing overhead costs.

core competencies. A bundle of skills and technologies that enable a company to provide a particular benefit to customers that gives it competitive differentiation.

corporate governance. The system by which organizations are directed and controlled. Its structure specifies the distribution of rights and responsibilities among different participants in the organization and spells out the rules and procedures for making decisions on corporate affairs. The result is the structure through which corporate objectives are set and through which the means of obtaining those objectives and monitoring performance are achieved.

cost behavior. How a cost reacts or responds to changes in activity levels. Costs may be fixed, variable, or mixed.

cost center. A business segment whose manager has control over costs, but not over revenues or the use of invested funds.

cost driver. A factor that causes overhead costs, such as machine hours, labor hours, or computer time.

cost management. The application of managerial accounting concepts, methods of data collection, data analysis, and data presentation so that relevant information can be provided for purposes of planning, monitoring, and controlling costs.

cost object. Anything for which cost data are desired, such as products, product lines, customers, jobs, or organizational subunits.

cost of capital. The average rate of return that a corporation must pay to its long-term creditors and shareholders for the use of their funds.

cost of goods manufactured. Manufacturing costs associated with goods that are completed and become available for sale during the period.

current cash debt coverage ratio. A measure of liquidity that can be calculated by dividing cash provided by operating activities by average current liabilities.

current ratio. A measure commonly used to evaluate a company's liquidity and short-term debt-paying ability that can be calculated by dividing total current assets by total current liabilities.

customer relationship management. A combination of customer information systems, personalization systems, content management systems, and campaign management systems.

debt to asset ratio. A measure of solvency that shows the percentage of total assets financed with borrowed funds; calculated by dividing total liabilities by total assets.

decentralization. The process of delegating decision making authority throughout an organization by empowering managers at various operating levels within the organization to make key decisions relating to their area of responsibility.

depletion. The process of allocating the cost of a natural resource over its estimated useful life.

depreciation. The process of allocating the cost of an item of property, plant, and equipment over its estimated useful life.

differential cost. Any difference in cost between two alternative courses of action under consideration. Also referred to as relevant cost.

differential revenue. Any difference in revenue between two alternative courses of action under consideration. Also referred to as relevant revenue.

direct allocation method. A method of allocating service department costs to operating departments that allocates all service department costs directly to those operating departments without recognizing any services provided to other service departments.

direct cost. Any cost that can be easily and conveniently traced to a specified cost object.

direct labor. Any manufacturing labor costs that can be conveniently and easily traced to individual units of product.

direct labor budget. A detailed plan that shows the labor requirements needed to meet projected production requirements over a specified period of time.

direct materials. Any manufacturing materials costs that can be conveniently and easily traced to individual units of product.

direct materials budget. A detailed plan that shows the amount of raw materials that must be purchased during a specified period of time in order to meet production needs and provide for the desired level of ending raw materials inventory.

directing. Mobilizing employees to carryout plans and perform routine operations.

discretionary fixed cost. Any fixed cost that is considered to be relatively easy to adjust because it arises from annual decisions by management to spend in certain fixed cost areas such as advertising, employee development, or research and development.

duration driver. In activity-based costing, a measure of the amount of time required to perform an activity.

earnings per share (EPS). A measure of the net income earned on each share of common stock outstanding; calculated by dividing net income minus preferred stock dividends by the average number of common shares outstanding during the year.

economic value added (EVA). A concept similar to residual income used for performance evaluation purposes.

enterprise governance. The set of responsibilities and practices exercised by executive management and the board of directors with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that the organization's resources are used responsibly. It is wider than, and inclusive of, corporate governance.

feedback. Accounting and nonaccounting reports and other information that assist managers in monitoring performance and in focusing on problems or opportunities that might otherwise go unnoticed.

financial accounting. Accounting activities concerned with providing information to external users such as stockholders, creditors, and government agencies.

finished goods. Units of output that have been completed but not yet sold to customers.

first-stage allocation. The process through which manufacturing overhead costs are assigned to activity cost pools in an activity-based costing system.

fixed cost. A cost that remains constant in total, within a relevant range, even as activity changes. On a per unit basis, it varies inversely with changes in activity.

flexible budget. A budget that has been designed to cover a range of activity and that can be used to develop budgeted costs at any point within that range to compare to actual costs incurred.

free cash flow. The amount of cash available from operations after adjusting for capital expenditures and cash dividends paid; calculated by subtracting capital expenditures and cash dividends paid from operating cash flow.

horizontal analysis. A technique for evaluating a series of financial statement data over a period of time to determine the increase or decrease that has taken place, expressed as either an amount or a percentage.

ideal standards. Standards in a standard costing system that allow for no machine breakdowns or other work interruptions and that require peak efficiency at all times.

incremental cost. Any change in cost between two alternative courses of action under consideration.

incremental revenue. Any change in revenue between two alternative courses of action under consideration.

indirect cost. Any cost that cannot be easily and conveniently traced to a specified cost object.

indirect labor. Labor costs of janitors, supervisors, materials handlers, and other factory workers that cannot be conveniently and easily traced to individual units of product.

indirect materials. Materials costs for small items such as glue and nails that are an integral part of a finished product but cannot be conveniently and easily traced to individual units of product.

intellectual capital. Comprised of human capital (knowledge, skills, and experience), relational capital (external relationships including customers and suppliers), and structural capital (knowledge that remains within the entity and includes procedures and systems).

internal control. The entire system of controls, both financial and nonfinancial, established in order to provide reasonable assurance of effective and efficient operation, internal financial control, and compliance with laws and regulations.

internal rate of return. The rate or return promised by a capital investment project over its useful life. It is the discount rate at which the present value of all cash inflows exactly equals the present value of all cash outflows so that the net present value is zero.

inventory turnover ratio. A liquidity measure that shows the number of times on average that inventory is sold during the period; calculated by dividing cost of goods sold by the average inventory during the period.

investment center. A business segment whose manager has control over costs, revenues, and invested funds.

joint cost. Any cost incurred up to the split-off point in a process that produces joint products.

joint products. Two or more items that are produced using a common input.

just-in-time (JIT). A production and inventory control system where raw materials are purchased and units of output are produced only on an as-needed basis to meet customer demand.

keep or drop decision. Decision resulting from a relevant cost analysis concerning whether a product line or segment should be retained or dropped.

knowledge management. A collective phrase for a series of processes and practices used by organizations in order to increase their value by improving the effectiveness of the generation and application of intellectual capital.

liquidity. The ability of a company to pay its short-term obligations as they are expected to become due within the next year or operating cycle.

liquidity ratios. Measures of the company's ability to pay its short-term obligations as they become due and to meet unexpected needs for cash as they arise.

make or buy decision. Decision resulting from a relevant cost analysis concerning whether an item should be produced internally or purchased from an outside source.

management by exception. A system of management that involves setting standards for various operating activities and then comparing actual results to these standards, with any significant differences being brought to the attention of management as "exceptions."

managerial accounting. Accounting activities concerned with providing information to managers for planning and control purposes and for making operating decisions.

manufacturing overhead. Any manufacturing cost that cannot be classified as direct labor or direct materials.

manufacturing overhead budget. A detailed plan that shows all production costs except direct materials and direct labor that are expected to be incurred over a specified time period.

marketing or selling costs. Any cost associated with securing customer orders and delivering the finished product or service into the hands of the customer.

master budget. A summary of the organization's plans in which specific targets are set for sales, production, distribution, and financing activities; generally includes a cash budget, budgeted income statement, and budgeted balance sheet.

merchandise purchases budget. A detailed plan that shows the amount of goods a merchandising company must purchase from suppliers during the period in order to cover projected sales and provide desired levels of ending inventory.

mission and vision statements. Statements that aim to describe the purpose of an organization, define its success, outline its strategy, and share its values.

mixed cost. A cost that contains both fixed and variable elements.

net operating income. Income before interest and income taxes have been deducted.

net present value. The difference between the present value of all cash inflows and the present value of all cash outflows associated with a capital investment project.

operating assets. Cash, accounts receivable, inventory, plant and equipment, and any other assets held for productive use by an organization.

operating department. Any department or segment within an organization within which the central purposes of the organization are carried out.

operating lease. An agreement allowing one party (the lessee) to use the asset of another party (the lessor) in an arrangement accounted for as a rental.

opportunity cost. The potential benefit that is foregone when one alternative is selected over another.

outsourcing. The use of external suppliers as a source of finished products, components, or services. Also known as contract manufacturing or subcontracting.

payback period. The length of time that it takes for a capital investment project to fully recover its initial cash outflows from the cash inflows that it generates.

performance report. A detailed report that compares budgeted data with actual results.

period cost. Any cost that is reported on the income statement in the period in which it is incurred or accrued; such costs consist of marketing and administrative expenses.

planning. Selecting a course of action and specifying how it will be implemented.

planning and control cycle. The flow of management activities through planning, directing and motivating, controlling, and then back to planning again.

postaudit. The follow-up that occurs after a capital investment project has been approved and implemented to determine whether expected results are actually realized.

practical standards. Standards in a standard costing system that allow for normal machine downtime and other work interruptions, and which can be attained through the reasonable but highly efficient efforts by the average worker.

predictive accounting. The use of process information to project future financial and nonfinancial performance.

present value. The value today of an amount to be received at some future date after taking current interest rates into account.

prime cost. Cost of the inputs to the production process. It is the sum of direct materials costs plus direct labor costs.

process reengineering. Improving operations by completely redesigning business processes in order to eliminate unnecessary steps, minimize errors, and reduce costs.

product cost. Any cost associated with the purchase or manufacture of goods; not reported on the income statement until the period in which the finished product is sold; such costs consist of direct materials, direct labor, and manufacturing overhead.

production budget. A detailed plan that shows the number of units that must to be produced during a period in order to cover projected sales and provide desired levels of ending inventory.

profit center. A business segment whose manager has control over costs and revenues but not over invested funds.

profit margin ratio. A measure of profitability that shows the percentage of each sales dollar that flows through to net income; calculated as net operating income divided by net sales.

profitability index. The ratio of the present value of a capital investment project's cash inflows to the present value of its cash outflows.

profitability ratios. Measures of the income or operating success of a company over a given period of time, usually one year.

quality of earnings. Refers to the level of full and transparent information that is provided to external users of a corporation's financial statements.

ratio. An expression of the mathematical relationship between two or more financial statement items that may be expressed as a percentage, a rate, or a proportion.

ratio analysis. A technique for evaluating financial statements that expresses the relationship among two or more selected financial statement items.

raw materials. Materials that are used to manufacture a finished product.

reciprocal allocation method. A method of allocating service department costs to operating departments that gives full recognition to interdepartmental services.

required rate of return. The minimum rate of return that any capital investment project must yield in order for it to be considered acceptable.

residual income. The net operating income of an investment center that exceeds its minimum required return on operating assets.

responsibility accounting. An accountability system under which managers are held responsible for differences between budgeted and actual results only for those items of revenue and expense over which they can exert significant control.

responsibility center. Any business segment whose manager has control over cost, revenue, invested funds, or all three.

return on equity. A measure of profitability that shows the efficiency with which operating assets were used to generate returns to stockholders; can be calculated by dividing net operating income by average common stockholders' equity.

return on investment (ROI). A measure of profitability that shows the efficiency with which operating assets were used to generate operating profits; can be calculated by dividing net operating income by average operating assets or by multiplying profit margin by asset turnover rate.

sales budget. A detailed schedule that shows the expected sales for coming periods, typically expressed both in dollars and in units.

second-stage allocation. The process by which activity rates are used to apply costs to products and customers in activity-based costing.

segment. Any part of an organization that can be evaluated independently of other parts and about which management seeks financial data.

segment margin. The amount remaining after a segment's traceable fixed costs have been subtracted from its contribution margin. It represents the amount available after a segment has covered all of its own traceable costs.

sell or process further decision. Decision resulting from a relevant cost analysis concerning whether a joint product should be sold at the split-off point or sold after further processing.

selling and administrative expense budget. A detailed plan that shows the expected selling and administrative expenses that will be incurred during a specified period of time.

service department. Any department that provides support or assistance to operating departments but does not directly engage in production or other operating activities.

simple rate of return. The rate of a return on a capital investment project that is determined by dividing its annual accounting net operating income by the initial investment required. Also referred to as accounting rate of return.

solvency. The ability of a company to pay interest as it comes due and to repay the principal amount of a debt at its maturity.

solvency ratios. Measures of the ability of a company to pay its long-term obligations as they become due and to survive over time.

special order. Any one-time order that is not considered part of the organization's normal ongoing business.

split-off point. The point in the manufacturing process where some or all of the joint products can be recognized and sold as individual products.

static budget. A budget created prior to the onset of the budgeting period that is valid only for the planned activity level.

step allocation method. A method of allocating service department costs to operating departments that allocates service department costs to other service departments as well as to operating departments in a sequential fashion that typically starts with the service department that provides the greatest amount of service to other departments.

strategic enterprise management. An approach to strategic management that focuses on creating and sustaining shareholder value through the integrated use of best practice modeling and analysis techniques, technologies, and processes in support of better decision making.

strategic planning. The formulation, evaluation, and selection of strategies for the purpose of preparing a long-term plan of action in order to attain objectives.

sunk cost. Any cost that has already been incurred or that cannot be changed by any decision made currently or in the future.

theory of constraints. A management approach that emphasizes the importance of managing bottlenecks caused by scarce resources.

times interest earned ratio. A solvency measure of the company's ability to meet interest payments as they come due that can be calculated by dividing income before interest expense and income taxes by interest expense.

total manufacturing cost. Cost of all inputs to the production process during a period. It is the sum of direct materials used, direct labor incurred, and manufacturing overhead.

total quality management. An integrated and comprehensive system of planning and controlling all business functions so that products and services are produced that meet or exceed customer expectations.

traceable fixed cost. Any fixed cost that is incurred because of the existence of a particular business segment.

transaction driver. In activity-based costing, a simple count of the number of times an activity occurs.

treasury management. The corporate handling of all financial managers, the generation of internal and external funds for the business, the management of currencies and cash flows, and the complex strategies, policies, and procedures of corporate finance.

value chain. The major business functions that add value to an organization's products or services, such as research and development, product design, manufacturing, marketing, distribution, and customer service.

value-based management. The process of searching for and implementing those activities that will contribute most to increases in shareholder value.

variable cost. A cost that varies in total, within a relevant range, in direct proportion to changes in activity. On a per unit basis, it remains constant as activity levels change.

variable cost ratio. The ratio of total variable costs to total revenues, or the ratio of unit variable cost to unit selling price. It is used in cost-volume-profit analysis.

variable costing. A costing method that treats only the variable manufacturing costs (direct materials, direct labor, and variable overhead) as product costs while it treats fixed overhead as a period cost. It is also referred to as direct costing.

vertical analysis. A technique for evaluating financial statement data that expresses each item in a financial statement as a percent of a base amount.

work in process. Units of product that have been only partially completed and will require further work before they are ready for sale to customers.

working capital (net). A measure used to evaluate a company's liquidity and short-term debt-paying ability that can be calculated by subtracting total current liabilities from total current assets.

XBRL. A computer language for financial reporting known as Extensive Business Reporting Language. It allows companies to publish, extract, and exchange financial information through the Internet and other electronic means in a standardized manner.

zero-based budget. A method of budgeting that requires managers each year to justify all costs as if the programs involved were being proposed for the first time.

About the Author

Ron Rael, Leadership Coach, is an award-winning speaker and facilitator who uses advanced learning techniques to deliver measurable, bottom-line results. Ron's highly customized High Road™ training systems shape existing and emerging leaders. Based upon his accomplishments as a business executive, Ron helps companies turn their drive for success into real results of employee satisfaction, customer retention, and internal cooperation.

How Ron's High Road™ perspective serves you:

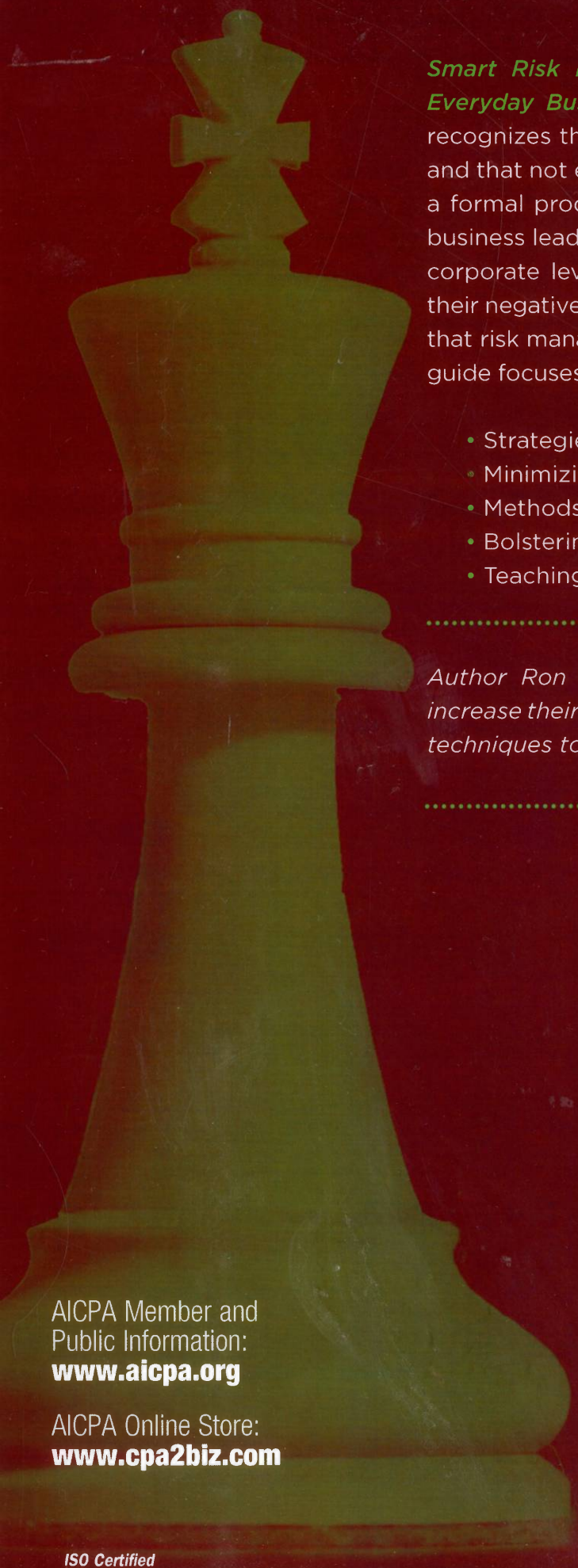
- He makes the invisible, visible in your leadership program.
- He opens your eyes to what you don't see.
- He brings forth wisdom you have yet to uncover.
- He tells you the truth about your business's personality.
- He coaches, counsels, guides, and finally holds you accountable for your integrity.

Serving you as your High Road™ coach, Ron is an observer, advisor, and mentor providing honest feedback and the tools that build cooperation and trust. Your team is quickly working together with an attitude of interdependence because of Ron's emphasis on resilience, open communication, and mutual accountability.

As a coach to individuals, Ron strikes a balance between encouragement and accountability, assisting the emerging leader to write and implement a personal action plan for growth and improvement. You quickly discover and capitalize on your internal motivation to succeed and become more courageous.

Ron has personally trained thousands of leaders and business professionals throughout the United States and Canada. He is well-known for his fun and original approach to learning. He develops caring, courageous, and compelling leaders worldwide.

His book (now in bookstores) *13½ Strategies for Winning the Budget Wars* takes a unique approach to doing an honest budget. The AICPA offers nine courses authored by Ron through www.cpa2biz.com.



Smart Risk Management: A Guide to Identifying and Reducing Everyday Business Risks is designed for any decision-maker who recognizes that too much effort in controlling risks hurts innovation and that not enough control is wasteful and expensive. By describing a formal process for defining and handling risk, this book provides business leaders with tools to manage risk at both the individual and corporate level. Readers will learn to confidently take risks, reduce their negative effects, increase opportunities for innovation, and prove that risk management is more than an insurance policy. This valuable guide focuses on the following topics, as well as many others:

- Strategies for analyzing risk
- Minimizing risks' downsides
- Methods to recover quickly from negative impacts of risk
- Bolstering your ability to accept more risk with confidence
- Teaching others to take risks and be more innovative

Author Ron Rael, CPA, who has helped hundreds of companies increase their profits with his strategies, provides you with 50 different techniques to greatly enhance your risk management skills.

AICPA Member and Public Information:
www.aicpa.org

AICPA Online Store:
www.cpa2biz.com

ISBN 978-0-87051-749-5

9 780870 517495

ISO Certified

029884