CHAPTER 1

Introduction to Risk Management

To avoid repeating the painful failures in risk management that occurred during the global financial crisis of 2007 to 2009 (also known as the Great Recession), it is essential for today's business, IT, risk, compliance, and audit managers to understand the big picture of risk management and to accept that risk management goes along with every position in business, technology, accounting, and finance. This is also true for many managers in the not-for-profit and government sectors.

This book is designed to provide an introduction to financial risk management, including operational, credit, market, reputational, liquidity, solvency, legal, and portfolio risk. These categories are based on the Basel II Capital Accords used by the global banking industry, but are applicable to all enterprises and organizations.

You will acquire an understanding of the major areas of risk exposure that all organizations, both public and private, face in operating in today's complex global marketplace. Risk management is an essential element in all business activities.

You will also be provided with actionable methods, techniques, and tools to improve risk management in your organization. This includes the basics of conducting risk assessments and risk alignments.

Definition of Risk and Financial Risk Management

Definitions of *risk* typically refer to the possibility of a loss or an injury created by an activity or a person. Risk management seeks to identify, assess, and measure risk and then develop countermeasures to handle it—not to eliminate risk.

Financial risk management applies a systematic and logical approach to uncertainties in operations, reputation, credit, liquidity/solvency, portfolios, and markets. Without risk management, an organization would simply rely on luck to avoid disasters. Risk management typically means seeking to mitigate and minimize the impact of risk, which is fundamentally different from avoiding it entirely. An organization that is completely risk averse is not likely to be attractive to investors and may be doomed to ultimately fail.

Risk should not be viewed as inherently bad. All opportunities come with some degree of risk—two sides of the same coin.

Gambling, Investment Risk, Chance, and Probability

Gambling can be defined as playing a game of chance for money or stakes. It requires one to risk money, or other things of value, on the outcome of something involving chance. *Investing* is to put money or other things of value to use by an expenditure or purchase in an investment vehicle that offers profitable returns. An investment vehicle may be a security or derivative, and can range from an asset-backed security to a stock or bond. An investment vehicle is used to make a profit on capital invested in it.

There is not a clear distinction between gambling and investment risk, but one can argue that risk taking in investments is good and adds capital to markets and thus contributes to society. One can also argue that gambling is inherently bad and adds limited value to society, although it does support some economies—Native American tribes, Las Vegas, and so on. Ironically, gambling risks are more identifiable,

measurable, and quantifiable than investment risks. Investment risks can be mitigated, whereas gambling risks typically cannot.

Risk can also be viewed as *probability* or the *chance* of making an incorrect decision. The risks of making a wrong decision are unique to the decision being made and may be realized only if a wrong decision is made. Unlike gambling, chance, and probability, risk management offers mitigation techniques.

Enterprise and Systemic Risk

Enterprise risk can be viewed as all processes that present risk to an organization. *Enterprise risk management (ERM)* comprises the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives. The goal of ERM is to provide a framework for risk management that:

- Identifies specific events, situations, and environments relevant to the organization's objectives and their applicable risks and opportunities.
- Assesses those risks in terms of their likelihood and consequences.
- Develops a risk mitigation strategy appropriate to the exposure (balancing the mitigation costs and benefits).
- Monitors and reports on the risk mitigation progress.

ERM mitigation strategies include:

- Avoidance: Ending the activities and processes that created the risk.
- Reduction: Reducing the likelihood and/or the consequences the risk through mitigation.
- Transference: Transferring or sharing a portion of the risk via insurance or other vehicles.
- Monitoring: Ongoing tracking and auditing of mitigation counter measures.
- Acceptance: Accepting the risk and taking no action.

Systemic risk is a term now in common use because of the global financial crisis and is typically used to explain the risk to an entire national economy and society caused by enterprise risk failures of large institutions deemed too big to fail. It is probably more accurate to describe these organizations as too interconnected to fail. Their size does present risk to the overall economy, but it is their ability to create a domino effect in which their failures cascade down into the failure of several other organizations that compels national treasuries to intervene. Lehman Brothers and AIG are the poster children for systemic risk failures in the last few years.

EXECUTIVE INSIGHT

Systemic Risks Increase after the Global Financial Crisis

Systemic and enterprise risks are distinct but very much interrelated. The catastrophic enterprise risk failures of Lehman Brothers, AIG, and several global banks presented a systemic risk to the United States and several Euro Zone economies. Interestingly, the large majority of my Santa Clara University MBA students expressed concerns that the global financial crisis has

increased our systemic risk for two reasons. First, national governments have set a bad precedent of bailing out large corporations rather than letting them fail, and thus have rewarded their reckless risk taking. Second, the major consolidation of banks reduces the distribution of risk so that the surviving banks present an even larger systemic risk. Their concerns are well founded, especially because there has been little government action to address the huge unregulated credit default swap (CDS) and derivatives markets or to reform rating agencies.

Relationships among Governance, Risk, and Compliance

Just as risk and opportunity go hand in hand, risk goes hand in hand with governance and compliance. *Governance* is the relationship between those who govern and those whom they govern over. *Compliance* is the system of laws, regulations, and standards that control the governance and risk management process. It may be best to understand the compliance side of this triangle as a hierarchy with laws at the top and enterprise-level tasks at the bottom.

- Laws are created by national, state, and local legislatures.
- Regulations are created by agencies and typically make the rules that public and private companies must adhere to.
- Standards are created by regulatory agencies and international organizations that establish the audit standards by which compliance to regulations are validated.
- Enterprises create policies (higher level) and procedures (detailed level) to comply with standards by which they will be audited.
- Procedures lead to a large number of specific and auditable tasks to enforce policies, standards, regulations, and laws.

TIPS AND TECHNIQUES

The Hierarchy of Laws, Regulations, and Standards

A common misconception is that enterprises only comply with national and state laws. Although this is true on the surface, enterprises are measured by how they pass statutory (legally required) audits against compliance and risk standards and frameworks (addressed in Chapter 2). These audits are conducted by government regulators and external auditors. Standards are the detailed and actionable face of laws and regulations. In the case of the Sarbanes-Oxley Act (less than 30,000 words), public companies in the United States must follow the audit standards from the Public Company Accounting Oversight Board (PCAOB). The PCAOB's Audit Standards 1, 3, 4, 5, and 6 total more than 50,000 words. Auditors create audit questionnaires, process charts, risk/control metrics, audit test scripts, findings, and remediations that typically run into thousands of pages. Enterprises create general policies and detailed procedures to pass PCAOB and other statutory audits. Each procedure comprises a multitude of required tasks and supporting documentation.

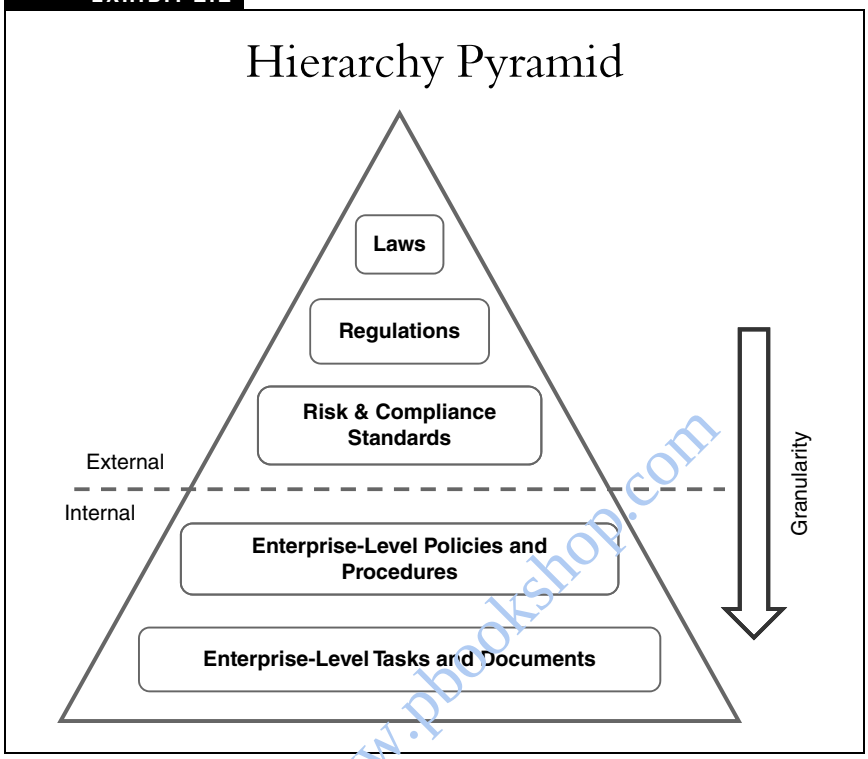
The pyramid graphic in Exhibit 1.1 is a good way to view this hierarchy.

Risk Management and Internal Controls

The process that an organization, its internal auditors, its external auditors, and its regulators would typically follow to validate the effectiveness of internal controls that impact financial reports would typically include these steps:

- Identify business processes, especially those impacting financial reporting.
- Identify the risks associated with each process.

EXHIBIT 1.1



- Identify the internal controls used to mitigate the risks for each process.
- Create a hierarchy of business processes, risks, and controls.
- Identify the tests to be used in determining the effectiveness of the internal controls.
- Test the internal controls and publish findings.
- Provide an opinion (findings) as to the effectiveness of the controls.
- If the controls are found to be ineffective, recommend changes (remediation) and retest the controls—alternatively, change the process to reduce the risk and retest.
- Create and maintain a documentation library of the processes, risks and controls, tests, findings, remediations, process narratives, and process flow charts.

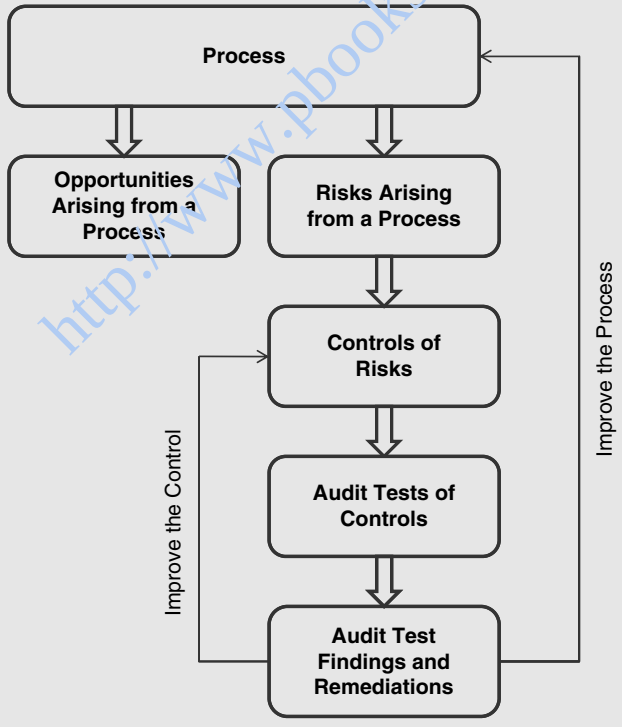
TIPS AND TECHNIQUES

The Relationship among Processes, Risks, and Controls

Exhibit 1.2 is a simple means to visualize the relationship among processes, risks, and controls. These exist in a many-to-many relationship, which means one control can cover multiple risks and one risk can be covered by multiple controls. One process may come with multiple risks as well.

EXHIBIT 1.2

Relationship among Processes, Risks, and Controls



Risk Management in Corporations

Under Western legal models, there are three actors in corporations: directors, employees, and shareholders. Each has a role in risk management.

- *Directors* provide the oversight and stewardship over all corporate assets, both human and otherwise. This includes aligning the corporations risk appetite with its risk exposure, yet it is common for Western boards to put the burden of risk management on executives. Evidence of this is that risk committees at the board level exist in few corporations.[1]
- *Employees* do the day-to-day work of managing the corporation's resources and assets. They execute the risk strategy and practices of the corporation. Notice that corporate executives are not treated under the law as separate actors but as employees.
- *Shareholders* provide the money in the form of risk capital and share risk equal to their investments. Under the Anglo-American model, shareholders have little say in risk management and can only vote with their feet—selling their shares. Their involvement in corporate operations is typically limited to interaction with the board, and not with corporate employees. Large institutional investors have exerted greater demands over boards, but typically not in the areas of risk management.

A corporate executive's approach to risk management is heavily influenced by the corporate governance model in place. In the United States and United Kingdom, agency theory is preferred; in Germany, Japan, and Islamic nations, stewardship theory is preferred. Under the Western agency theory, executives are driven to achieve short-term objectives that tend to translate into greater risk taking. In good times, the agency approach can achieve greater growth and profitability than the more conservative stewardship approach. In bad times, the conservatism of the stewardship approach can help to insulate a corporation

from major losses. The major elements of each approach can be summarized as follows:

Executives	Agency Theory (e.g., U.S., U.K.)	Stewardship Theory (e.g., Islam, Germany, Japan)
Act as	Agents	Stewards
Behavior model is	Self-serving, individualistic	Pro-organizational, collectivistic
Motivated by	Their own interests	Their principals' interests
Alignment with principals' interest	Limited or divergent	Closely aligned

The agency approach comes with a chronic and significant issue known as the principal/agent problem. This is a classic dilemma for any organization that is not family-owned and run. Employees are agents with self-serving interests. Principals (owners and corporate board members) attempt to align the interest of their employees (agents) and the organization (principals) with a wide variety of compensation models. The problem can never be solved, only mitigated. When the interests of principals and agents are poorly aligned, corporations can be exposed to material risk through shortsighted and reckless employee behavior or outright fraud. The global crisis exposed multiple examples of highly compensated executives who drove their corporations over a cliff, in part because their compensation models contained few incentives to act as stewards protecting the long-term interests of their employers.

Evolution of Risk Management

Financial risk management as a discipline has progressed since the pivotal year of 1921, when Frank Knight published his *Risk, Uncertainty, and Profit,* and John Maynard Keynes published his *A Treatise on*

Probability. Knight pioneered the notion that uncertainty, which cannot be measured, is different from risk, which is measurable. Keynes pioneered the mathematical and philosophical foundations of risk management. Keynes argues for a greater reliance on perception and judgment when considering probabilities and warns against an over-reliance on numbers.

In 1956, Russell Gallagher published his *Risk Management: A New Phase of Cost Control* in the *Harvard Business Review*, arguing that a professional insurance manager should also be a risk manager. Because of the nature of its business, the insurance industry was the first to embrace professional risk management with its concern for avoiding unaffordable potential losses—actuarial risk.

In the 1980s, new risk societies were created to promote risk management—the Society for Risk Analysis in Washington and the Institute for Risk Management in London. Their efforts have made the concepts of risk assessment and risk management well understood in business and government circles.

In the 1990s, the U.K.'s Cadbury and Turnbull committees issued reports advocating that corporate boards take responsibility for setting risk management policies, for assuring that the organization understands all its risks, and for accepting oversight for the entire process.

It was also in the 1990s that the title chief risk officer (CRO) was first used by GE Capital to describe a manager who is responsible for the totality of risk exposure to an organization. Chief risk officers and risk managers are now commonplace in the financial services industry and they are spreading into other industries.

Risk management as a distinct discipline may be fairly new, but risk management is as old as man. Noah is an early example of risk mitigation techniques in practice—building a giant ark of no commercial or recreational value in the belief that he was not crazy and really had talked to God. Good managers have always understood that risk management must be addressed in every opportunity pursuit.

Ethical and Moral Foundations to Risk Management

Historically, investors in most companies were individuals ranging from the very rich to the working class. Over recent decades, however, institutional investors representing insurance companies; banks; investor groups; and mutual, hedge, and pension funds have become dominant players in the market. Institutional investors have been able to advocate for stronger corporate governance and oversight. Although oversight has improved, it has not necessarily improved the voice of small investors, or improved risk management. The growth of mutual funds and pension plans has given small investors at least an indirect voice.

The need for institutional investors to access equity capital on a global level has increased the demand for improved governance, typically manifested through improved financial transparency, accountability, and representation of minority shareholder interests. The process has increased demand for what is commonly referred to as *tone-at-the-top*—corporate boards and executives providing the stewardship, culture, and organization committed to corporate governance.

Tone-at-the-top, as the jurist said about pornography, is hard to define, but you know it when you see it. The fundamental issue around tone-at-the-top may come down to the basic ethics and morality of those in positions of corporate power. If there is no moral and ethical foundation to the tone-at-the-top, then rules, regulations, and sanctions will ultimately fail. Morally bankrupt wrongdoers are often too clever and powerful to be caught, at least initially.

These are some suggestions to help establish an ethical tone-at-the-top approach to risk management:

- The organization's board and executive management have embraced ethical risk management as a continuous process that is critical to meeting the organization's objectives.

- The board of directors has demonstrated its full support for risk management as an integral part of the organization—there is a management consensus as to the main drivers around risk.
- The board and senior management have designed an overarching risk management policy that includes objectives and responsibilities.
- The board has created a risk committee at the board level.
- The board has ensured the alignment among the firm's business objectives, revenue drivers, and its risk exposure and appetite. Risk environment and risk appetite are aligned.
- There is a chief compliance and risk officer (one person) at a minimum and ideally both a risk officer and a compliance officer (two people).
- The organization has an ongoing process to assess and track the benefits of improved risk management.
- The organization understands its main risk weaknesses and has compared them to their peer organizations and the best-in-class organizations.
- The organization has invested in high-caliber management with the skills, training, compensation rewards, and resources to improve risk management.
- The board has endorsed financial rewards for whistleblowers as a means to expose unethical and illegal behavior.
- The board draws from the management talent pool of the country and region so that it is sufficiently diverse as to age, sex, and ethnicity. (There is positive correlation between increased female board representation and improved governance.)[2]

EXECUTIVE INSIGHT

Tone-at-the-Top at Lehman Brothers

Richard Fuld, chairman of the board (CoB) and chief executive officer (CEO) of now-defunct Lehman Brothers, testified to Congress in October 2008 after the collapse of his firm a month earlier. When asked if he thought his $354 million salary over the past five years was justified in light of Lehman's shareholders being wiped out and the loss of 20,000 jobs, Fuld responded that his compensation was determined by the compensation committee. The Congressman snapped back asking who the compensation committee reported to. Fuld calmly responded that they reported to him as chairman of the board.

Fuld's holding both the CEO and CoB positions is known as *duality*, which is common in the United States, but much less common and discouraged in much of the world. CEO/CoB duality creates obvious conflicts of interests in which Fuld could orchestrate his own compensation package with few checks and balances. CEO/CoB duality also challenges risk management checks and balances with one person responsible for short-term execution (CEO) and long-term stewardship (CoB).

EXECUTIVE INSIGHT

Lessons from Miyamoto Musashi, Japan's Greatest Samurai

The problems with risk management can be summarized in the teachings of the legendary Samurai master swordsman, Miyamoto Musashi, in his *Book of the Five Rings*.

Musashi, who lived in fifteenth-century Tokugawa, Japan, won more than 30 duels and is considered by many as the greatest Samurai swordsman of all time. He retired to a life of solitude and wrote a short book about sword-fighting techniques that many of us believe applies to business in general and specifically to risk management. In Musashi's business, risk failure meant death or disgrace.

There are at least two great risk lessons from Miyamoto Musashi.

1. Never take a hard focus on the point of your opponent's sword. The attack will never come from the point of the sword, directly in front of you, but from some other direction. (This is true in Western fencing as well.) He advises to take a soft focus in order to prepare for an attack in any direction. The reactionary and myopic nature of regulatory reforms did little to prevent the largest financial crisis since the 1930s because reforms were focused on the point of the sword.
2. Never favor one weapon—master all of them. If you do have a favorite, you will be defeated when forced to use your least favorite weapon. Risk managers must master all the tools at their disposal as well.

Risk is like this. The biggest threats never come from the most visible point of attack. Risk managers in most organizations are experts in specific areas of risk, for example, credit risk in banking, but the global financial crisis involved a failure of every major type of risk. Few organizations were masters of each area of risk management and fewer still were able to take a holistic approach to their enterprise risk.

Effective risk management must take a more holistic approach because the next risk problem will not look like the last one and may come from a completely different direction. What does this mean to you in business, assuming you are not assigned to address one specific area of risk? A few thoughts:

- Do not assume government regulations, rating agencies, or financial audits will protect you.
- Do not assume risk experts understand multiple areas of risk and how they impact one another, sometimes referred to as risk complexity. (The global crisis involved failures in each type of risk we address in this text.)
- You are more expert in complex risk management than you may think. Remember the lessons of Miyamoto Musashi to keep a soft focus and follow the guidance from the 9/11 Commission that concluded the attacks were caused by a lack of imagination on the part of those responsible for our protection. Keeping a soft focus and your imagination will help to identify and address the next Black Swan coming your way.

Summary

Although we use the Basel II framework to categorize the various types of risk, there is no universally accepted framework for risk management. Just as medicine has become highly specialized, risk management requires specialization for each type of risk. The skills required of a loan officer in credit risk are quite different than those required by an IT security manager in such areas of operational risk as external and internal fraud. This book does not attempt to dive deep into each area of risk, but does provide an introduction and points you in the right direction for additional information. Like medicine, the disciplines in risk management are progressing rapidly, indicating that continuing education is essential. Common techniques in use today did not exist 10 to 20 years ago.

The global financial crisis has taught us that even the most sophisticated risk management techniques and tools in the hands of well-funded professionals can be seriously flawed, especially when obsessive greed trumps common sense. The fundamental problem with risk management comes from what are often called Black Swans, outlier events, rare but disastrous risk management failures that are extremely difficult to predict using statistical forecasting and other historical observations.

Failures in risk management typically result in a reactionary regulatory and mitigation process that addresses the problem in a myopic fashion. This typically does little to prevent or curtail the next crisis. An example is the enactment of the Sarbanes-Oxley Act (SOX), which was designed in response to the financial reporting abuses and scandals of the late 1990s.[3] A related example is the Basel II capital accords that were in force for many European Union (EU) banks at the onset of the crisis.[4] Unfortunately SOX did nothing to prevent major U.S. banks from failing after they reported strong quarterly and annual results. Basel II failed in a similar fashion for the EU banks.

Notes

1. See Chapter 24 in Anthony Tarantino and Deborah Cernauskas, *Financial Risk Management, Six Sigma and Other Next Generation Techniques* (Hoboken, NJ: John Wiley & Sons, 2006).
2. Ibid.
3. See Chapter 9 in Sanjay Anand and Anthony Tarantino, *Sarbanes Oxley in Leading Economies* (Upper Saddle River, NJ: Prentice-Hall, 2010).
4. See Chapter 41 in Anthony Tarantino, *Governance, Risk, and Compliance Handbook* (Hoboken, NJ: John Wiley & Sons, 2008).