1

WHY RISK MANAGEMENT?

> The internal audit activity should assist the organization by identifying and evaluating significant exposures to risk and contributing to the improvement of risk management and control systems.
>
> IIA Standard 2110

INTRODUCTION

Internal auditing has grown tremendously over the years to reflect its new high-profile position in most larger organizations. It has shifted from back-office checking teams to become an important corporate resource. The focus on professionalism and objectivity has driven the new-look auditor toward high-impact work that can really make a difference. The key development that has underpinned this change relates to the shift from enforcing controls on employees to using an assessment of risk to empower management and their staff to establish meaningful controls over their business. This move from must-do to want-to control cultures has allowed employees more scope to innovate and experiment.

Unfortunately, in the past, robust risk management processes have not always been in place. The rapid change programs of the 1980s and '90s meant that many organizations were likened to speeding trains that would leave behind anyone who was not bold enough to jump on board and hang on for dear life. Investors expected quick returns, while competition was about being the first to bring new or improved products to the marketplace—or at least give that impression. The resultant crashes and scandals that rebounded throughout the last decade underpinned the lack of clear direction or ethical values that could be described as the much-needed rail signals and brakes—to continue our train analogy.

Reckless trading against the backdrop of the cutthroat competition of the 1990s continued into 2000 and beyond, before the regulators started to get tough. The old governance models of a select board of high achievers

gathered around a powerful CEO, whose only accountability was to publish financial accounts that had been reviewed by a friendly auditor, could not cope with the new business dynamic. In this type of environment, regulations were seen as obstacles to be sidestepped. Corporate lawyers were often used to design roadmaps to allow the executive teams to weave a path through legal provisions and industry-specific regulations. Societal concerns came to a head in 2002, with the publication of the Sarbanes-Oxley Act, to enshrine personal responsibility at the top of each company to adhere to the rules and demonstrate that this is the case. The link between risk management and corporate governance has been explored by the Institute of Internal Auditors (IIA):

> Risk management is a fundamental element of corporate governance. Management is responsible for establishing and operating the risk management framework on behalf of the board.[1]

In the past, control frameworks have helped in setting standards, but they often acted as basic benchmarks to be checked off against and often ended up as just checks in the Compliance Box, something that is done and then filed away—until the same time next year. Nowadays, the new focus is firmly on risk—to the business, executives, and stakeholders. Several societal concerns appear at the forefront of this idea of risk, including the risks that:

- Published accounts are misleading.
- Performance information is fudged.
- Regulatory disclosures are not supported by sound evidence.
- Senior executives are making uninformed assertions about the adequacy of controls over financial reporting and compliance procedures.
- The corporate asset base is not properly protected from waste, loss, attack, or natural disaster.
- The corporate reputation militates against customer loyalty.
- Operations and processes are inefficient and inflexible.
- The wrong people are being promoted and recruited.
- The organization is failing to meet the changing expectations of customers, the marketplace, and stakeholders generally.

Attempts to address these issues have led organizations in the direction of Enterprise Risk Management (ERM). That is a wholesale approach to identifying and managing risk across all aspects of the business—from a strategic standpoint. As each risk changes in impact and urgency, so

does the organization respond to ensure that any damage is limited and opportunities are exploited through using gaps in the market thrown up by new risks. In fact, the main feature of a successful enterprise is its ability to anticipate and deal with global risks more efficiently than other similar organizations. In this scenario where the stakes are so high, the role that is carved out by the internal auditor becomes all the more important. If ERM is to be a key driver for success, the various parties that affect the ERM framework that is built to address risk across the business become a fundamental concern. Where each party has a clear role, there is a need to discharge the precise responsibilities of each of these roles. Any shortfalls may lead to problems. The choices made by the Chief Audit Executive, in the context of the audit approach to ERM, are likewise important, and nothing should be left to chance.

If organizations faced no risk, there would be no need to employ internal audit staff. The organization would always be in complete control, and there would be no need to review, adjust, realign, or even implement internal controls. The auditor exists because plans do not always go as intended, and things don't always appear as they really are. The auditor is needed to ensure that the organization understands its risks and has taken steps to both handle foreseeable problems and seize potential advantages. Advising, helping, cajoling, and issuing warnings are all tools that may be employed by the auditor to put risk on the agenda and ensure that it is given proper consideration. This combination of effort to achieve a risk-smart workforce means that the auditor is fast becoming what some now refer to as a critical friend to executives, management, and employees generally.

Before we launch our first model, we need to outline the formal definition of *internal auditing* from the IIA:

> Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.[2]

As is clear from this definition, internal auditing is firmly rooted in the risk management, control, and governance agenda. Dave Richards, President of the IIA, presented at the IIA's Enterprise Risk Management and Control Self-Assessment* Conference in Las Vegas, Nevada, on September 9, 2004, which is reported as follows:

*Control Risk Self-Assessment (CRSA) is also called Control Self-Assessment (CSA); the two terms are interchangeable.

> Richards highlighted key ERM and CSA trends, including legislative movements around the world emphasizing the need for risk management as well as signs that internal auditors are becoming more proactive in the use of risk-assessment processes. Although CSA has not been fully embedded in many organizations, he said ERM is becoming known as a key ingredient to good governance, and internal auditors should promote its adoption and progression. In Richards' closing comments he encouraged the audience by saying, "It couldn't be a better time to be in the internal audit profession," and challenged participants to advocate risk management processes within their organizations while keeping internal audit standards and basic principles at the forefront of their audit activities.[3]

This sets the challenge: To help and support management as they struggle with establishing good risk management in the organization, while ensuring that the rigorous provisions of audit standards are retained. *Risk management* is defined by the IIA as:

> A process to identify, assess, manage, and control potential events or situations, to provide reasonable assurance regarding the achievement of the organization's objectives.[4]

Enterprises include all public and private-sector organizations, and *enterprise risk management* is described as:

> A structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives.[5]

We will also be devoting some time to a landmark document on ERM, which was launched by the Committee of Sponsoring Organizations (COSO) on September 29, 2004. COSO consists of five major professional associations in the United States and was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting. All further references in this book to COSO ERM relate to the 2004 COSO ERM framework. Further information on COSO and their publications can be viewed on their Web site at *www.coso.org*. COSO provides the following commentary in its foreword to ERM guidance:

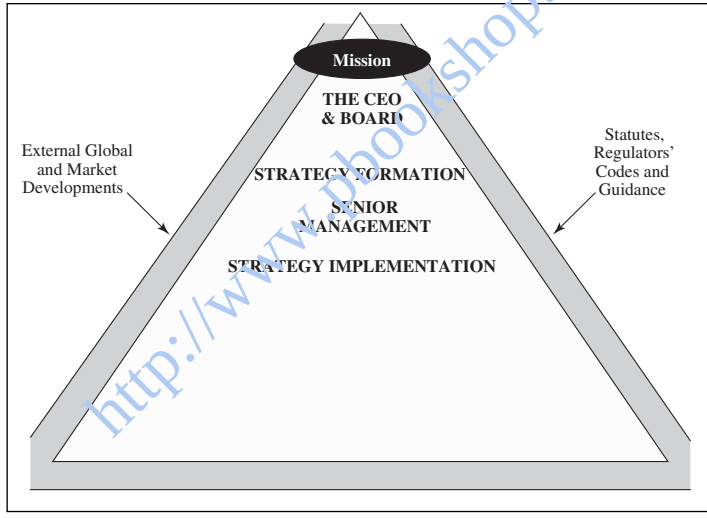
> The need for an enterprise risk management framework, providing key principles and concepts, a common language, and clear direction and guidance, became even more compelling. COSO believes this Enterprise Risk Management—Integrated Framework fills this need, and expects it

will become widely accepted by companies and other organizations and indeed all stakeholders and interested parties.[6]

RISK MANAGEMENT FRAMEWORK MODEL: PHASE ONE

Our first model looks at the way risk management resides in an organization. We start at the top of an enterprise with the position of the CEO and the board and the way they respond to the pressure to ensure good corporate governance in Figure 1.1.

Figure 1.1 Risk Management Framework Model: Phase One



Each aspect of the model is described below.

External Global and Market Developments

Risk is inherent in the way global events shift in the economy, including changing interest rates, international developments, and the fluctuating movement of capital. Meanwhile, markets are constantly changing as consumer demand alters and competitors enter or leave the marketplace. Public-sector services are also affected by constant changes in the demands

and expectations of society. This sense of uncertainty has been summed up by COSO:

> Enterprises operate in environments where factors such as globalization, technology, restructurings, changing markets, competition and regulation create uncertainty.[7]

Statutes, Regulations, Codes, and Guidance

Governance codes and company legislation can be generic or industry specific, and they create additional demands on enterprises—normally in response to heightened expectations from society, or as a result of corporate scandals that revealed a need to tighten up on existing regulations. The most famous of the more recent laws arrived several years ago in the guise of Sarbanes-Oxley, with the resulting impact on companies listed on the New York Stock Exchange and NASDAQ. An assortment of local state laws also add to the compliance framework within which enterprises must operate. Some professions, such as law, medical practice, and accounting, provide various codes of conduct and specific regulations that must be adhered to by their practicing members. Within this context, governance is about the way organizations conduct themselves and administer their affairs. The IIA's definition of *governance* is:

> The combination of processes and structures implemented by the board in order to inform, direct, manage and monitor the activities of the organization toward the achievement of its objectives.[8]

Most significant organizations understand the need to respond properly to the wider demands of society as expressed through the regulators. The foreword to the COSO ERM addresses this important point:

> The period of the framework's development was marked by a series of high-profile business scandals and failures where investors, company personnel, and other stakeholders suffered tremendous loss. In the aftermath were calls for enhanced corporate governance and risk management, with new law, regulation, and listing standards.[9]

Business performance goes hand in hand with regulatory performance, as described by one large retail company:

> Our size and global reach present extraordinary opportunities, but also present additional complexity in dealing with an ever-changing variety

> of laws and regulations. Keeping pace with changes in the regulatory environment is a challenge for management, but we are committed to do so. We continually monitor our legal and regulatory performance, and will upgrade internal systems or change the way we do business when necessary in order to assure compliance.[10]

The Mission

The risk management framework is driven by what the organization is trying to achieve, which, at its highest level, is the overall mission. For example, the mission of the Ford Motor Company is stated as:

> We are a global family with a proud heritage passionately committed to providing personal mobility for people around the world. We anticipate consumer need and deliver outstanding products and services that improve people's lives.[11]

Meanwhile, the company's future vision is:

> To become the world's leading consumer company for automotive products and services.[12]

Many corporate governance codes argue that corporate objectives should be enriched by ensuring that they also address wider societal concerns:

> In addition to their commercial objectives, companies are encouraged to disclose policies relating to business ethics, the environment and other public policy commitments.[13]

The reality of private, public-sector, and not-for-profit environments means that there can never be total certainty that the mission will always be fully achieved and make the vision a reality. Risk is about this lack of certainty, and it has been defined as follows:

> Risk is the chance of something happening that will have an impact on objectives. Therefore, to ensure that all significant risks are captured, it is necessary to know the objectives of the organization function or activity that is being examined.…Organizational success criteria are the basis for measuring the achievement of objectives, and so are used to identify and measure the impacts or consequences of risks that might jeopardize those objectives.[14]

The CEO and Board

The driving force for the enterprise is the CEO and board of directors. This is where the key decisions are made regarding the strategy that will transform the mission into firm results. The IIA defines a *board* in the following way:

> A board is an organization's governing body, such as a board of directors, supervisory board, head of an agency or legislative body, board of governors or trustees of a nonprofit organization, or any other designated body of the organization, including the audit committee, to whom the chief audit executive may functionally report.[15]

The board formulates strategy and employs executives, managers, staff, and appropriate resources to implement this strategy. The need for sound boards has been remarked on in the past:

> The three main problems at Enron were that the company had an accommodating and passive board, an unhealthy drive to meet earnings targets and—probably the most damaging quality—a penchant for hiring only the best and brightest and rewarding them lavishly if they proved they could innovate, innovate and innovate. Unfortunately, the dark side of innovation is fraud.[16]

Moreover, the board has a key role in overseeing the risk management process. COSO ERM has provided some direction in clarifying this role by suggesting the following oversight responsibilities:[17]

- Knowing the extent to which management has established effective enterprise risk management in the organization
- Being aware of and concurring with the entity's risk appetite
- Reviewing the entity's portfolio view of risk and considering it against the entity's risk appetite
- Being apprised of the most significant risks and whether management is responding appropriately

Strategy Formation

Our model suggests that the context for the development of a formal strategy is found within the global market forces and the relevant regulatory

framework for each individual organization. One short example of strategy formation comes from CalPERS, the California Employees' Retirement System, which provides retirement and health benefits:

> Our Strategic Plan provides our organization with a road map for meeting the retirement and health benefits needs of more than 1.4 million members and participating employers. It guides our business relations and interactions. Our business philosophy is straightforward. We are customer-focused, and our decision-making process is guided by value and quality.[18]

Senior Management

The next aspect of the model relates to senior management (i.e., the people who sit in the firing line to get the job done). The corporate strategy will result in various objectives that will need to be delivered to ensure that the organization is successful (i.e., the overall mission is achieved). Senior management run the business lines and are responsible for meeting key performance targets, commonly known as Key Performance Indicators (KPIs). COSO ERM builds on this theme and goes on to locate key responsibilities to senior managers.

> Managers guide application of ERM components within their sphere of responsibility, ensuring application is consistent with risk tolerances. In this sense, a cascading responsibility exists, where each executive is effectively a CEO for his or her sphere of responsibility.[19]

Strategy Implementation

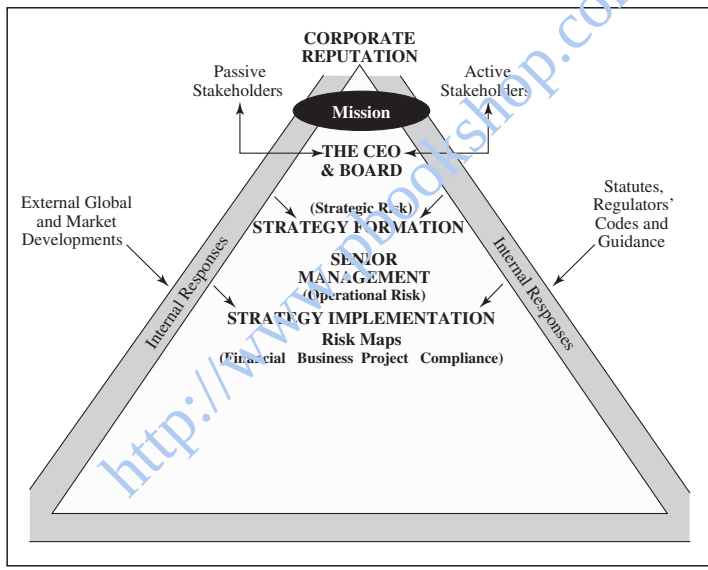
Managers are responsible for ensuring that their staff, systems, and budgets are applied to delivering the set strategy. They do this by breaking down the longer-term corporate strategy into more manageable shorter-term chunks that are handed out to their workforce and associates. The workforce is in effect the engine room of the organization. Empowering organizations allow people to make decisions on the front line and flex their responses to the needs of customers and clients. In terms of implementing solutions, the responsibilities of senior management have been outlined in the banking operational risk management framework, BASEL:

> Senior management should have responsibility for implementing the operational risk management framework approved by the board of directors.[20]

RISK MANAGEMENT FRAMEWORK MODEL: PHASE TWO

So far we have described an overall corporate arrangement that has a basic view of setting strategy and then implementing the various aspects of a more detailed plan to keep the workforce busy and productive. This rather one-dimensional version of the way businesses operate needs to become much more layered and colorful. The additional dimension that has emerged over the years relates to the need to isolate and understand risk. Our model is further enhanced in Figure 1.2 in recognition of this fact.

Figure 1.2 Risk Management Framework Model: Phase Two



Each new aspect of the model is described below.

Active Stakeholders

Over the years we have come to accept the role of stakeholders in corporate life. Active stakeholders have a direct influence over an organization, and in incorporated companies, this relates to shareholders who can vote on the board members and what they are paid for their services. Investors,

lenders, associates, partners, bankers, employees, and other parties each have an important influence on the organization. Likewise, institutional investors have a major role in holding a batch of voting shares in many large enterprises, whereas public-sector organizations are beholden to their public to ensure they deliver and deliver well. *Stakeholders*, in the context of risk management, are described in the Australian/New Zealand risk management standard:

> Those people and organizations who may affect, be affected by, or perceive themselves to be affected by a decision, activity or risk.[21]

Passive Stakeholders

There is a growing band of stakeholders that sits just outside of direct interfaces with specific enterprises, and this is what we mean by passive stakeholders. Local communities, the media, environmental groups, and people who are concerned about the behavior of large organizations may have no obvious influence over the board, but they do have some collective sway in the way the organization is seen by others. Increasingly, such pressure groups are able to influence businesses that are behaving badly or have not made a full assessment of their impact on local communities. The Australian/New Zealand risk management standard has something to say on this matter:

> Communication and consultation are important considerations at each step of the risk management process. They should involve a dialogue with stakeholders with efforts focused on consultation rather than a one-way flow of information from the decision maker to other stakeholders.[22]

There is an emerging theme based around the concept of corporate social responsibility that is starting to enhance the importance of all types of stakeholders.

Strategic Risk

Our model places strategic risk firmly on the corporate agenda. The risks from changing markets and the risk of failing to comply with various laws and rules, or meeting the needs of stakeholders, may mean the stated mission will not be achieved. Strategy takes on board these diverse risks and

ensures that they are addressed in such a way as to achieve the set objectives. This link is clearly defined in the Australian/New Zealand standard:

> Organizations that manage risk effectively and efficiently are more likely to achieve their objectives and do so at lower overall cost.[23]

The concept of strategic risk emphasizes strategic solutions. All organizations need to consider several matters that are encompassed in ERM:[24]

- Aligning risk appetite and strategy
- Enhancing risk-response decisions
- Reducing operational surprises and losses
- Identifying and managing cross-enterprise risks
- Providing integrated responses to multiple risks
- Seizing opportunities
- Improving deployment of capital

Many big risks confront all sorts of organizations, and global terrorism, rapid technological change, and the availability of good staff cannot always be underwritten by insurers. Many organizations have now moved toward internal insurance arrangements in the form of good risk management systems to reinforce the need for a sustainable business base. Returning to COSO ERM, several events may affect an organization, which can be classified as either external or internal factors:

- External factors:
  - Economic
  - Natural environment
  - Political
  - Social
  - Technological
- Internal factors:[25]
  - Infrastructure
  - Personnel
  - Process
  - Technology

Operational Risk

Strategy is a high-level concept that eventually gets filtered through to front-line operations. These operations need to address risk to the more detailed objectives that form the basis for the work of most middle managers and the actual workforce. Operational risk affects the day-to-day operational objectives, and each entity must deal with the important task of aligning operations across the entity:

> Enterprise risk management over operations focuses primarily on developing consistency of objectives and goals throughout the organization.[26]

International banks have already recognized the importance of operational risk management, and the Committee on Banking Supervision, Bank for International Settlement, have prepared guidance on operational risk management for the banking community. BASEL Principle One deals with the importance of operational risk:

> The board of directors should be aware of the major aspects of the bank's operational risks as a distinct risk category that should be managed, and it should approve and periodically review the bank's operational risk management framework.[27]

Risk Maps (Financial, Business, Project, and Compliance)

The next factor that we need to add to our model relates to the way generic risk is structured to fit the way the organization sees the world. There are many and varied perceptions of risks to an organization. We have broken down risk into various categories of financial, business, project, and compliance risk. In this way, a map can be drawn as to how these different types of risk run up, down, and through the organization. The COSO ERM viewpoint is that risk may be categorized as follows:

> Within the context of an entity's established mission or vision, management establishes strategic objectives, selects strategy, and sets aligned objectives cascading through the enterprise. This enterprise risk management framework is geared to achieving an entity's objectives, set forth in four categories:[28]
>
> 1. *Strategic*. High-level goals, aligned with and supporting its mission
> 2. *Operations*. Effective and efficient use of its resources

3. *Reporting*. Reliability of reporting
4. *Compliance*. Compliance with applicable laws and regulations

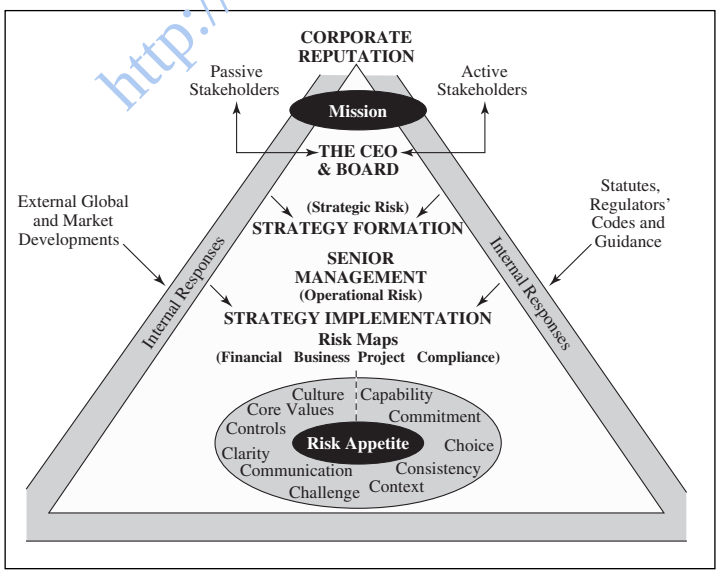
Risk maps attempt to track the way strategic and operational risk affects different parts of an organization. The Australian/New Zealand standard describes the way risk affects all parts of a business:

> Risk management can be applied at many levels in an organization. It can be applied at a strategic level and at tactical and operational levels. It may be applied to specific projects, to assist specific divisions or to manage specific recognized risk areas. For each stage of the process records should be kept to enable decisions to be understood as part of a process of continual improvement.[29]

RISK MANAGEMENT FRAMEWORK MODEL: PHASE THREE

Our model continues in Figure 1.3. Each new aspect of the model is described below.

Figure 1.3 Risk Management Framework Model: Phase Three



Risk Appetite

The concept of risk appetite appears next on the model, as it holds a central role in all risk management frameworks. As such, it warrants its own chapter, which appears later in the book (Chapter 4). Here we focus on 11 Cs that are important to understanding the way risk is perceived by an organization. Before we launch into these Cs we need to make clear that, in essence, risk appetite creates an unwritten contract between an organization and its stakeholders regarding the balance between exploiting opportunities and protecting the business and its reputation. If management moves too quickly to seize an opening, it may lose out in the long run. If it is too slow, it may also miss out in the long run. The concept of risk appetite runs across many risk standards, and for banks, risk appetite is seen as a major consideration:

> Banks should have policies, processes and procedures to control and/or mitigate material operational risks. Banks should periodically review their risk limitation and control strategies and should adjust their operational risk profile accordingly using appropriate strategies, in light of their overall risk appetite.[30]

Capability

Our first C relates to the capacity within an organization to understand and manage its risks. A short example will illustrate this point.

Case Study

The Cost of Low Capability

In one not-for-profit organization, there was no system of risk management in place and no record of how important decisions are made or plans approved. In fact, the one person who raised the issue was ridiculed or ignored by colleagues. A main feature of the corporate culture was poor role definition and the lack of clear objectives. The organization suffered for many years from fragmented teams and a reputation for vague and ill-defined services.

Commitment

The next C concerns the need for people to buy into the risk management concept (i.e., a commitment from the top that runs through the workforce), as in the following example.

CASE STUDY

Board-Level Sponsorship

In one public-sector body, a board-level Control Risk Self-Assessment (CRSA) sponsor is used to oversee the CRSA process and ensure that it is both effective and challenging. This person has to be satisfied that the risk workshops are well designed and that CRSA is being applied to the best effect within key parts of the business. The success criteria are defined as changed behaviors from staff as they take more ownership for their business processes and products.

Choice

Risk appetite resides in the choices that are made or not made on issues that have a significant impact on the success or otherwise of the business and is about the level of risk that remains after controls have been put in place. Decisions should be made based on the acceptability of this level of risk, described as follows:

> Residual risk is the risk that remains after treatment options have been identified and treatment plans have been implemented. It is important that stakeholders and decision makers are aware of the nature and extent of the residual risk. The residual risk should therefore be documented and subjected to monitor and review.[31]

Consistency

The next C suggests that the organization should apply a consistent approach to the way it manages risk (i.e., it fits with the way people behave at work):

> The risk management process should be customized for the organization, its policies, procedures and culture taking into account the review process.[32]

Context

Risk appetite should be seen within the context of the way an organization operates and deals with its customers and other stakeholders. Establishing the right context is therefore a prerequisite to establishing the right risk appetite:

> Communication and consultation are intrinsic to the process of risk management and should be considered at each step. An important aspect of "establishing the context" is to identify stakeholders and seek and con-

sider their needs. A communications plan can then be developed. This plan should specify the purpose or goal for the communication, who is to be consulted and by whom, when it will take place, how the process will occur, and how it will be evaluated.[33]

Challenge

Risk management should not lead to a bunker mentality in which people become obsessed with a multitude of risks that have a remote bearing on the business. It should lead to an empowered workforce that is able to take charge of its priorities and decide what works best at the sharp end, as demonstrated in this example.

Case Study

The Risk Management Challenge

In one commercial company, risk management was sold as a chance for each local office to secure some degree of autonomy from head office control. So long as they adhered to the basic control and compliance systems, they were free to implement local initiatives after they had been formally risk-assessed. Some managers performed risk assessments using a team approach, whereas others carried out a basic review, or analytical survey. Team-based CRSA workshops were designed to last less than an hour at a time. Internal audits would help these local managers understand and meet the set criteria, as well as reviewing their efforts. Risk maps and detailed registers were compiled by the chief risk officer (CRO) from regular interviews with the managers. The really good managers performed well, whereas poor ones did not last long. The middle range received a great deal of support from the CRO and chief internal auditor in understanding their risks.

Communication

The corporate risk appetite can only be understood if people around the organization understand each other and their priorities. If the board has a view on what is acceptable behavior, it will need to paint this image for its stakeholders and employees, to support a common understanding of risk appetite:

> Communication between an organization and its external stakeholders allows an organization to develop an association with its community of interest, and to establish relationships based on trust.[34]

Clarity

Clarity of objectives, clear accountabilities, and clear risk triggers all underpin the way risk is perceived and addressed. In an attempt to clarify risk owners and risk appetite, the way accountabilities are set and applied will need to be reviewed, as in the following example.

Case Study

Doing Your Homework

In a national realty company, a great deal of time was spent in defining delegated authority levels at each branch based on head office policies on managing clients and negotiating deals. This exercise was deemed necessary before an effective risk management system could be established.

Controls

Controls are an important equation in setting risk appetite. Controls are set against high levels of inherent risk to reduce this risk down to an acceptable level. The extent to which an operation is controlled depends on an organization's perspective of acceptable risk. The greater the focus on risk taking, to enhance market share, the less the emphasis on fixed controls. Controls nowadays are moving toward being more flexible and organic and entirely responsive to changing risks. *Controls* are defined as follows:

> Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.[35]

Controls respond to risk, and COSO ERM suggest that several matters should be considered when deciding on the application of controls:[36]

- Effects of potential response on risk likelihood and impact—and which response options align with the entity's risk tolerances
- Costs versus benefits of potential responses
- Possible opportunities to achieve entity objectives going beyond dealing with the specific risk

Core Values

Risk appetite is closely aligned to corporate values. When we decide on what is acceptable in the way we work, this requires a value judgment. Acceptability is about appropriateness (i.e., what fits under the circumstances). An organization that has spent a great deal of time and effort to define its core values has a better chance of defining its risk appetite:

> To be most effective, risk management should become part of an organization's culture. It should be embedded into the organization's philosophy, practices and business processes rather than be viewed or practiced as a separate activity. When this is achieved, everyone in the organization becomes involved in the management of risk.[37]

Culture

The next part of the risk appetite model relates to a matter that has already been alluded to—that of culture. Many commentators view governance as a meeting of performance-driven success criteria and conformance-based constraints (i.e., delivering the goods but in a right and proper manner). This balance is affected by the type of corporate culture in place, ranging from gung ho to stickler for rules employee attitudes:

> Root causes (of risk) can include facets of an organizational culture such as ingrained processes and practices or paradigms that need to change to successfully treat a risk from occurring (and reoccurring). Sources of risk that flow on from attitudes within organization culture, cannot be treated successfully unless changes are made to these facets.[38]

The importance of corporate culture can have a wide-ranging effect on the way risk is perceived and dealt with, as shown in the following example.

Case Study

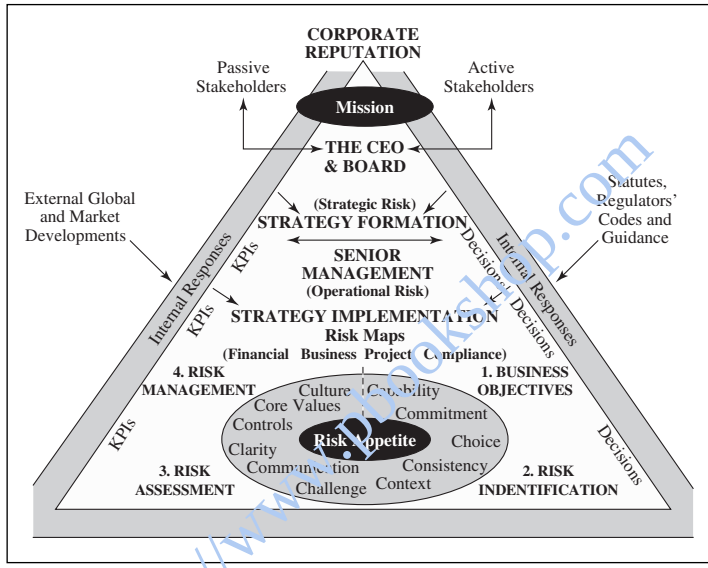
Working within the Culture

In a listed company, risk management was applied without the use of the terms *risk, control,* or *risk management.* The driver was based around better business, and this focused on achieving better results and more responsive teams that managed their work proactively. A decision was made to apply risk concepts in a way that suited the way people worked and communicated with each other. The main issue was centered around learning and improving, and the risk assessments were applied with this in mind (e.g., much is made of near misses and how they can be avoided in future).

RISK MANAGEMENT FRAMEWORK MODEL: PHASE FOUR

Our model continues in Figure 1.4. Each new aspect of the model is described below.

Figure 1.4 Risk Management Framework Model: Phase Four



Senior Management

In most organizations, management makes the most impact on whether the corporate objectives will be achieved or not. If senior management does not adopt the risk management concept wholeheartedly, there is little chance that a systematic analysis of risk will be undertaken and applied to steering the business through rocky waters. This point is brought out in the Australian/New Zealand standard:

> The directors and senior executives are ultimately responsible for managing risk in the organization. All personnel are responsible for managing risks in their areas of control. This may be facilitated by:[39]
>
> - Specifying those accountable for the management of particular risks or categories of risk, for implementing treatment strategies and for the maintenance of risk controls;

- Establishing performance measurement and reporting processes and ensuring appropriate levels of recognition, reward, approval and sanction.

Business Objectives

All risk frameworks have the term *objectives* set somewhere in their central components. This is a key point. Risk as a vague concept that floats above an organization is often associated with disasters and accidents (i.e., things that appear out of the blue and are largely uncontrollable). In this sense, risk is something that one suffers in silence and not as we suggest something that can be anticipated and managed. We can view risk as anything that affects our objectives, and in this way encourage people to take charge of their work by viewing many risks as potentially controllable, or at least potentially minimized. The use of ERM in promoting the achievement of objectives has been documented by the IIA:

> ERM can make a major contribution towards helping an organization manage the risks to achieving its objectives. The benefits include:[40]
>
> - Greater likelihood of achieving those objectives
> - Consolidated reporting of disparate risks at board level
> - Improved understanding of the key risks and their wider implications
> - Identification and sharing of cross business risks
> - Greater management focus on the issues that really matter
> - Fewer surprises or crises
> - More focus internally on doing the right things in the right way
> - Increased likelihood of change initiatives being achieved
> - Capability to take on greater risk for greater reward
> - More informed risk-taking and decision-making

Risk Identification

Once the need for effective risk management has been recognized, we come to the task of isolating all possible risks. This is before we have weighed each risk to determine whether it is substantial or not. Risk identification is the process of capturing all those risks that affect the relevant business objectives. This task is included in our model as an important step in promoting better-run organizations. The following short example will help illustrate this point.

CASE STUDY

Being Risk Smart

In one division, the goal was to get a risk-smart attitude into the workforce. Risk concepts were built into team meetings, and people started to think ahead and plan for the consequences of their actions. People were told not to accept any blame for problems that lay elsewhere, but to find out what needed fixing and delegate it to those who were responsible to act. For example, a staff shortage lies with those whose job it is to ensure staffing quotas and absence planning. Most of the problem lay in poor communications between the resource planning team and the front-line managers. A workshop between the two offices was held to isolate the risks, consequences of these risks, and ways forward. This approach is now used whenever an interface-based problem impacts service delivery.

COSO ERM uses the concept of an *event* to drive the risk identification stage of the risk management cycle:

> An event is an incident or occurrence emanating from internal or external sources that affects implementation of strategy or achievement of objectives. Events may have a positive or negative impact, or both.[41]

Risk Assessment

The next part of the model relates to assessing known risks for their potential impact on an organization's ability to achieve its objectives. The most popular approach to risk assessment is to judge the possible impact of the risk if it materializes, and then judge the extent to which the risk is likely to occur. The results are normally plotted on a graph that measures these two axes, so that risks that fall in the top right corner (see Figure 1.5) would have a high impact on the objectives and are also likely to occur unless managed properly, as noted in the Australian/New Zealand standard, which describes the concept of *risk* as:

> The chance of something happening that will have an impact on objectives:[42]
>
> - A risk is often specified in terms of an event or circumstances that may flow from it.
> - Risk is measured in terms of a combination of the consequences of an event and their likelihood.
> - Risk may have a positive or negative impact.

Risk Management

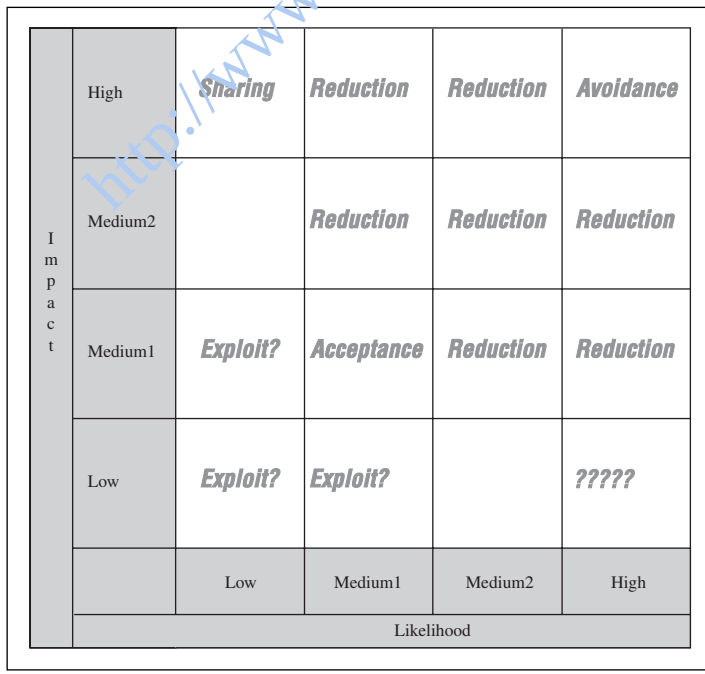
Risk management comes into the model in suggesting that having assessed our risks, we can then determine what steps to take to deal with anything that causes a concern (i.e., risk that is significant and likely to arise). COSO ERM supports that application of good risk management:

> Recent years have seen heightened concern and focus on risk management, and it became increasingly clear that a need exists for a robust framework to effectively identify, assess, and manage risk.[43]

There are many possible responses to different types and levels of risk, and the options are found in COSO ERM:[44]

- Avoidance
- Reduction
- Sharing
- Acceptance

Figure 1.5 Risk Management Responses



Avoidance and reduction strategies will tend to be associated with high-impact, high-likelihood risks, whereas sharing fits more with high-impact, low-likelihood risks. Acceptance will tend to focus on low-impact, low-likelihood risks—or where the cost of controls is prohibitive. Using the COSO ERM risk-response categories, we can set out the Impact/Likelihood chart and locate the appropriate strategies of Avoidance, Reduction, Sharing, and Acceptance.

One further risk response has been added to the chart in Figure 1.5, located toward the bottom left-hand corner, where both impact and likelihood are low. This is marked as Exploit, where parts of the business are encouraged to do more and be more innovative because their operations are far below the corporate risk appetite.

KPIs

Having used risk management to arrive at an action plan to improve controls or refine the way work is planned and performed, there is a need to consolidate these measures. The model is enriched by adding in the attachment of performance indicators to action plans that result from an assessment of risk. The facts of corporate life mean that any actions that are needed to grow the business must feed into personal or team performance targets to have any real chance of happening, but targets should be set with care:

> Setting realistic targets is sound motivational practice, reducing counter-productive stress as well as the incentive for fraudulent reporting.[45]

COSO ERM goes on to list 12 considerations that an organization may make in determining information requirements to underpin performance, in their guide on application techniques that accompanies the main guidance:[46]

- What are the key performance indicators for the business?
- What key risk indicators provide a top-down perspective of potential risks?
- What performance metrics are required for monitoring?
- What data are required for performance metrics?
- What level of granularity of information is needed?
- How frequently does the information need to be collected?
- What level of accuracy or rigor is needed?

- What are the criteria for data collection?
- Where and how should data be obtained?
- What data/information are present from existing processes?
- How should data repositories be structured?
- What data recovery mechanisms are needed?

Disclosures

The model turns now to the need for formal disclosures from the organization. Transparency relates to the obligations assumed from corporate accountability, and this point is brought out in the Australian/New Zealand standard:

> Sound risk management not only contributes to good governance, it also provides some protection for directors and office holders in the event of adverse outcomes. Provided risks have been managed in accordance with the process set out in the Standard, protection occurs on two levels. Firstly, adverse outcomes may not be as severe as they might otherwise have been. Secondly, those accountable can, in their defence, demonstrate that they have exercised a proper level of diligence.[47]

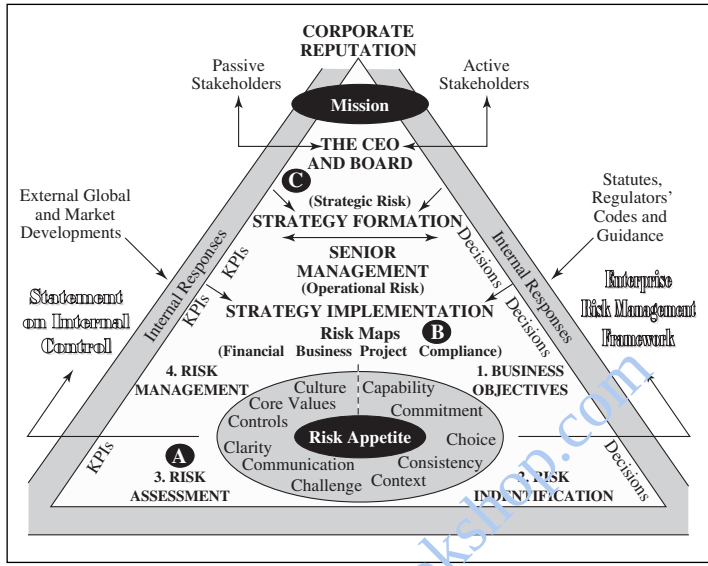
In the United States, the accountability regime that has emerged in the form of documented certifications over the last few years has been described by the IIA:

> The strength of all financial markets depends on investor confidence. Events involving allegations of misdeeds by corporate executives, independent auditors, and other market participants have undermined that confidence. In response to this threat, the U.S. Congress and a growing number of legislative bodies and regulatory agencies in other countries passed legislation and regulation affecting corporate disclosures and financial reporting. Specifically in the United States of America the Sarbanes-Oxley Act of 2002 (the Sarbanes-Oxley Act) enacted sweeping reform requiring additional disclosures and certifications of financial statements by principal executive and financial officers.[48]

RISK MANAGEMENT FRAMEWORK MODEL: FINAL

Our complete model is presented in Figure 1.6. Each new aspect of the model is described below.

Figure 1.6



Enterprise Risk Management Framework

One major aspect of the model is the all-consuming ERM framework that sweeps up all of the issues that have appeared so far in the model. ERM has been described as consisting of several activities as follows:[49]

- Articulating and communicating the objectives of the organization
- Determining the risk appetite of the organization
- Establishing an appropriate internal environment, including a risk management framework
- Identifying potential threats to the achievement of the objectives
- Assessing the risk (i.e., the impact and likelihood of the threat occurring)
- Selecting and implementing responses to the risks
- Undertaking control and other response activities
- Communicating information on risks consistently at all levels in the organization
- Centrally monitoring and coordinating the risk management processes and the outcomes and providing assurance on the effectiveness with which risks are managed

Good ERM means that an organization is in a better position to meet its set objectives while also complying with external regulations. It is about strong but sensible business continuity, against all types of problems that result from an uncertain environment. Good risk management is also required by the federal sentencing guidelines along with a system for ensuring compliance and reliable decision making. ERM is a significant business tool that comes into play whenever there is an objective to be met and whenever there is an understanding that there will always be some risk associated with achieving these objectives. Risk is not to be dreaded, but it is also not to be laughed at. There must be a careful balance between these two extremes, as explained in the following:

> If every possible risk that might occur in everyday life—never mind business life—could be recognized, anticipated, assessed and managed then life for all of us would be considerably easier than it is. However, it can't be done; it's an impossible dream. Besides, it's by taking risks that commercial organizations thrive and achieve their objectives. The existence of sufficient entrepreneurs to keep capitalism going year in, year out is testament to the turning of risk to good advantage—at least for most of the time.[50]

The important point to note is that a framework is needed to capture the essence of risk and risk management. A *risk framework* has been described as:

> A set of elements of an organization's management system concerned with managing risk. Management system elements can include strategic planning, decision making, and other strategies, processes and practices for dealing with risk.[51]

The Statement on Internal Control

Our model suggests that the CEO's Statement on Internal Control is related to the ERM process applied by an organization. Meanwhile, COSO ERM starts with a background to internal control:

> Among the outgrowths in the United States is the Sarbanes-Oxley Act of 2002, and similar legislation has been enacted or is being considered in other countries. This law extends the long-standing requirement for public companies to maintain systems of internal control, requiring management to certify and the independent auditor to attest to the effectiveness of those systems. Internal Control—Integrated Framework, which continues to stand the test of time, serves as the broadly accepted standard for satisfying those reporting requirements.[52]

The equation is fairly straightforward. Risks cause an element of uncertainty in meeting objectives. Controls help guard against risks that threaten an organization's ability to achieve its objectives. A good ERM process incorporates a good system of internal control and a mechanism to update controls as and when risks alter in type, impact, or likelihood. Moreover, any examination of a listed company by the Securities and Exchange Commission (SEC) into internal controls will start with the risk management system in operation. The bottom line of our model suggests that it is not possible to establish a sound system of internal control without first establishing an effective ERM process.

Monitoring

The entire risk management process must be kept up to date and vibrant. It must also be reviewed to ensure that it still does the job as intended. This all-important review is described as follows:

> Ongoing review is essential to ensure that the management plan remains relevant. Factors that may affect the likelihood and consequences of an outcome may change, as may factors that affect the suitability or cost of the treatment options. It is therefore necessary to repeat the risk management cycle regularly.[53]

Validation

Another aspect of our first risk management model is that risk activities need to be done in such as way that they can be validated, if necessary. This means there should be good documentation in place. Validation enables the board to set a mandate that designates that an effective risk management process will be put in place and in turn make several firm statements about their risk management policy, including the following lines:[54]

- The processes to be used to manage risk
- Accountabilities for managing particular risks
- Details of the support and expertise available to assist those accountable for managing risks
- A statement on how risk management performance will be measured and reported
- A commitment to the periodic review of the risk management system
- A statement of commitment to the policy by directors and the organization's executive

The use of formal documentation and validation has to be treated with care. The possible impact on employees should be properly managed. Records are essential, but there is a warning about their use:

> Records of communication and consultation will depend on factors such as the scale and the sensitivity of the activity.[55]

Improvement

Risk management must be set within a learning environment for it to be of any use. As such, our model includes the need to provide continuous improvement to the process for capturing real risks in a meaningful way. The Australian/New Zealand standard provides some of the most useful advice on this matter:[56]

> Incidents, accidents and successes provide a useful occasion to monitor and review risks and treatments and to gain insight on how the risk management process can be improved. The intention should be to adopt a systematic process to review causes of successes, failures and near misses to learn useful lessons for the organization. Ideally a systematic analysis process would be used. When successes and failures are analyzed, the questions to be answered are:
>
> - Did we previously identify and analyze the risks involved?
> - Did we identify the actual causes in risk identification?
> - Did we rate and assess risks and controls correctly?
> - Did the controls operate as intended?
> - Were the treatment plans effective?
> - If not, where could improvements be made?
> - Were our monitoring and review processes effective?
> - How could our risk management process in general be improved?
> - Who needs to know about these learnings and how should we disseminate these learnings to ensure that learning was most effective?
> - What do we need to do to ensure that failure events are not repeated but that successes are?

Continual Integration

The final part of the model captures the need to integrate risk management into the actual business systems and work methods. The business responds to risk, and it does this by incorporating threats and opportunities into the way it works:

> Management looks to align the organization, people, processes, and infrastructure to facilitate successful strategy implementation and enable the entity to stay within its risk appetite.[57]

SUMMARY

Risk management is now part of mainstream corporate life that touches all aspects of all types of organizations. One way to consider risk management is to go through the following five steps:

1. Consider risk management in its widest format as what most people call enterprise risk management (or enterprise-wide risk management).
2. Align ERM to the governance framework that incorporates the impact of stakeholders and the organization's corporate reputation.
3. Use strategy formation and implementation as the process by which risk is understood and addressed within the executive management of the business.
4. Set the operational risk cycle of business objectives, risk identification, risk assessment, and risk management within the framework set by ERM and the organization's management structure.
5. Superimpose the ERM framework and reporting on internal controls over these matters (1–4 above) and ensure that these two items can be formally documented and reported on to stakeholders.

Note that Appendix A contains checklists that can be used to assess the overall quality of the ERM system and also judge the type of audit approach that may be applied to supporting and reviewing the ERM process.

NOTES

1. Institute of Internal Auditors, UK & Ireland, Position Statement 2004, *The Role of Internal Audit in Enterprise-Wide Risk Management,* Conclusion.
2. Institute of Internal Auditors, definition of *internal auditing.*
3. Institute of Internal Auditors, *www.theiia.org*, October 2004.
4. Institute of Internal Auditors, Glossary of Terms.
5. Institute of Internal Auditors, Glossary of Terms (IIA, UK & Ireland).
6. Committee of Sponsoring Organizations, *Enterprise Risk Management*, September 2004, Forward to the Executive Summary.

7. *Ibid.*, p. 13.
8. Institute of Internal Auditors, Glossary of Terms.
9. Committee of Sponsoring Organizations, *Enterprise Risk Management*, September 2004, Foreword to the Executive Summary.
10. Walmart company, *www.walmart.com*, Letter from the Chairman of the Board, October 2004.
11. Ford company, *www.ford.com*, October 2004.
12. *Ibid.*
13. OECD Principles of Corporate Governance, "Organization for Economic Co-Operation and Development" (2004), p. 50.
14. Australian/New Zealand Standard: Risk Management Guidelines AS/NZS 4360:2004, p. 30.
15. Institute of Internal Auditors, Glossary of Terms.
16. Sharron Watkins, interviewed by Nancy Hala, "If Capitalists Were Angels," *The Internal Auditor* (April 2003): 38–43.
17. Committee of Sponsoring Organizations, *Enterprise Risk Management*, September 2004, Foreword to the Executive Summary, p. 83.
18. Californian Employees' Retirement System, *www.calpers.ca.gov*, October 2004.
19. Committee of Sponsoring Organizations, *Enterprise Risk Management*, September e2004, Foreword to the Executive Summary, p. 85.
20. BASEL Committee on Banking Supervision, Bank for International Settlement, February 2003, Principle 3.
21. Australian/New Zealand Standard: Risk Management Guidelines AS/NZS 4360: 2004, p. 6.
22. *Ibid.*, p. 11.
23. *Ibid.*, Foreword.
24. Committee of Sponsoring Organizations, *Enterprise Risk Management*, September 2004, Foreword to the Executive Summary, pp. 14–15.
25. *Ibid.*, p. 42.
26. *Ibid.*, p. 39.
27. BASEL Committee on Banking Supervision, Bank for International Settlement, February 2003, Principle 1.
28. Committee of Sponsoring Organizations, *Enterprise Risk Management*, September 2004, Executive Summary.
29. Australian/New Zealand Standard: Risk Management Guidelines AS/NZS 4360:2004, p. 8.
30. BASEL Committee on Banking Supervision, Bank for International Settlement, February 2003, Principle 6.
31. Australian/New Zealand Standard: Risk Management Guidelines AS/NZS 4360:2004, p. 86.
32. *Ibid.*, p. 27.
33. *Ibid.*, p. 21.
34. *Ibid.*, p. 23.
35. Institute of Internal Auditors, Glossary of Terms.
36. Committee of Sponsoring Organizations, *Enterprise Risk Management*, September 2004, Foreword to the Executive Summary, p. 56.
37. Australian/New Zealand Standard: Risk Management Guidelines AS/NZS 4360:2004, Foreword.

38. *Ibid.*, p. 74.
39. *Ibid.*, p. 27.
40. Institute of Internal Auditors, UK & Ireland, Position Statement 2004, *The Role of Internal Audit in Enterprise-Wide Risk Management*, Conclusion.
41. Committee of Sponsoring Organizations, *Enterprise Risk Management*, September 2004, Foreword to the Executive Summary.
42. Australian/New Zealand Standard: Risk Management Guidelines AS/NZS 4360:2004, p. 4.
43. Committee of Sponsoring Organizations, *Enterprise Risk Management*, September 2004, Foreword to the Executive Summary.
44. *Ibid.*, p. 55.
45. *Ibid.*, p. 30.
46. *Ibid.*, p. 75.
47. Australian/New Zealand Standard: Risk Management Guidelines AS/NZS 4360:2004, p. 11.
48. Institute of Internal Auditors, Practice Advisory 2120.A1-3.
49. Institute of Internal Auditors, UK & Ireland, Position Statement 2004, *The Role of Internal Audit in Enterprise-Wide Risk Management*, Conclusion.
50. Neil Cowan, *Corporate Governance That Works* (Prentice Hall, Pearson Education South Asia Pte Ltd., 2004), p. 37.
51. Australian/New Zealand Standard: Risk Management Guidelines AS/NZS 4360:2004, p. 5.
52. Committee of Sponsoring Organizations, *Enterprise Risk Management*, September 2004, Foreword to the Executive Summary.
53. Australian/New Zealand Standard: Risk Management Guidelines AS/NZS 4360:2004, p. 22.
54. *Ibid.*, p. 27.
55. *Ibid.* (extracts only), p. 11.
56. *Ibid.*, p. 93.
57. Committee of Sponsoring Organizations, *Enterprise Risk Management*, September 2004, Foreword to the Executive Summary, p. 40.