

Enterprise risk management— integrated framework

Executive summary
September 2004

Copyright © 2004 by the Committee of Sponsoring Organizations of the Treadway Commission.

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

All rights reserved. For information about reprint permission and licensing please call (201) 938-3245. A permissions request form for emailing request is available at www.aicpa.org/copyright.htm. Otherwise, requests should be submitted in writing and mailed to Permissions Editor, AICPA, Harborside Financial Center, 201 Plaza Three, Jersey City, NJ 07311-3881.

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Oversight

COSO Chair

American Accounting Association

American Institute of Certified Public Accountants

Financial Executives International

Institute of Management Accountants

The Institute of Internal Auditors

Representative

John J. Flaherty

Larry E. Rittenberg

Alan W. Anderson

John P. Jessup
Nicholas S. Cyprus

Frank C. Minter
Dennis L. Neider

William G. Bishop, III
David A. Richards

Project Advisory Council to COSO

Guidance

Tony Maki, Chair
Partner
Moss Adams LLP

James W. DeLoach
Managing Director
Protiviti Inc.

John P. Jessup
Vice President and Treasurer
E.I. dePont de Nemours and
Company

Mark S. Beasley
Professor
North Carolina State University

Andrew J. Jackson
Senior Vice President of
Enterprise Risk Assurance Services
American Express Company

Tony M. Knapp
Senior Vice President and Controller
Motorola, Inc.

Jerry W. DeFoor
Vice President and Controller
Protective Life Corporation

Steven E. Jameson
Executive Vice President,
Chief Internal Audit & Risk Officer
Community Trust Bancorp, Inc.

Douglas F. Prawitt
Professor
Brigham Young University

PricewaterhouseCoopers LLP

Author

Principal contributors

Richard M. Steinberg
Former Partner and Corporate
Governance Leader (presently
Steinberg Governance Advisors)

Frank J. Martens
Senior Manager, Client Services
Vancouver, Canada

Miles E.A. Everson
Partner and Financial Services
Finance, Operations, Risk and
Compliance Leader
New York

Lucy E. Nottingham
Manager, Internal Firm Services
Boston

Foreword

Over a decade ago, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued *Internal Control – Integrated Framework* to help businesses and other entities assess and enhance their internal control systems. That framework has since been incorporated into policy, rule, and regulation, and used by thousands of enterprises to better control their activities in moving toward achievement of their established objectives.

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. In 2001, COSO initiated a project, and engaged PricewaterhouseCoopers, to develop a framework that would be readily usable by managements to evaluate and improve their organizations' enterprise risk management.

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. 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.

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.

This *Enterprise Risk Management – Integrated Framework* expands on internal control, providing a more robust and extensive focus on the broader subject of enterprise risk management. While it is not intended to and does not replace the internal control framework, but rather incorporates the internal control framework within it, companies may decide to look to this enterprise risk management framework both to satisfy their internal control needs and to move toward a fuller risk management process.

Among the most critical challenges for managements is determining how much risk the entity is prepared to and does accept as it strives to create value. This report will better enable them to meet this challenge.

John J. Flaherty
Chair, COSO

Tony Maki
Chair, COSO Advisory Council

Executive summary

The underlying premise of enterprise risk management is that every entity exists to provide value for its stakeholders. All entities face uncertainty, and the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. Enterprise risk management enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value.

Value is maximized when management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks, and efficiently and effectively deploys resources in pursuit of the entity's objectives. Enterprise risk management encompasses:

- Aligning risk appetite and strategy – Management considers the entity's risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.
- Enhancing risk response decisions – Enterprise risk management provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance.
- Reducing operational surprises and losses – Entities gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.
- Identifying and managing multiple and cross-enterprise risks – Every enterprise faces a myriad of risks affecting different parts of the organization, and enterprise risk management facilitates effective response to the interrelated impacts, and integrated responses to multiple risks.
- Seizing opportunities – By considering a full range of potential events, management is positioned to identify and proactively realize opportunities.
- Improving deployment of capital – Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

These capabilities inherent in enterprise risk management help management achieve the entity's performance and profitability targets and prevent loss of resources. Enterprise risk management helps ensure effective reporting and compliance with laws and regulations, and helps avoid damage to the entity's reputation and associated consequences. In sum, enterprise risk management helps an entity get to where it wants to go and avoid pitfalls and surprises along the way.

Events – risks and opportunities

Events can have negative impact, positive impact, or both. Events with a negative impact represent risks, which can prevent value creation or erode

existing value. Events with positive impact may offset negative impacts or represent opportunities. Opportunities are the possibility that an event will occur and positively affect the achievement of objectives, supporting value creation or preservation. Management channels opportunities back to its strategy or objective-setting processes, formulating plans to seize the opportunities.

Enterprise risk management defined

Enterprise risk management deals with risks and opportunities affecting value creation or preservation, defined as follows:

Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

The definition reflects certain fundamental concepts. Enterprise risk management is:

- A process, ongoing and flowing through an entity
- Effected by people at every level of an organization
- Applied in strategy setting
- Applied across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risk
- Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite
- Able to provide reasonable assurance to an entity's management and board of directors
- Geared to achievement of objectives in one or more separate but overlapping categories

This definition is purposefully broad. It captures key concepts fundamental to how companies and other organizations manage risk, providing a basis for application across organizations, industries, and sectors. It focuses directly on achievement of objectives established by a particular entity and provides a basis for defining enterprise risk management effectiveness.

Achievement of objectives

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:

- Strategic – high-level goals, aligned with and supporting its mission
- Operations – effective and efficient use of its resources
- Reporting – reliability of reporting
- Compliance – compliance with applicable laws and regulations.

This categorization of entity objectives allows a focus on separate aspects of enterprise risk management. These distinct but overlapping categories – a particular objective can fall into more than one category – address different entity needs and may be the direct responsibility of different executives. This categorization also allows distinctions between what can be expected from each category of objectives. Another category, safeguarding of resources, used by some entities, also is described.

Because objectives relating to reliability of reporting and compliance with laws and regulations are within the entity's control, enterprise risk management can be expected to provide reasonable assurance of achieving those objectives. Achievement of strategic objectives and operations objectives, however, is subject to external events not always within the entity's control; accordingly, for these objectives, enterprise risk management can provide reasonable assurance that management, and the board in its oversight role, are made aware, in a timely manner, of the extent to which the entity is moving toward achievement of the objectives.

Components of enterprise risk management

Enterprise risk management consists of eight interrelated components. These are derived from the way management runs an enterprise and are integrated with the management process. These components are:

- Internal Environment – The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
- Objective Setting – Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.
- Event Identification – Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.
- Risk Assessment – Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.
- Risk Response – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite.
- Control Activities – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
- Information and Communication – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.

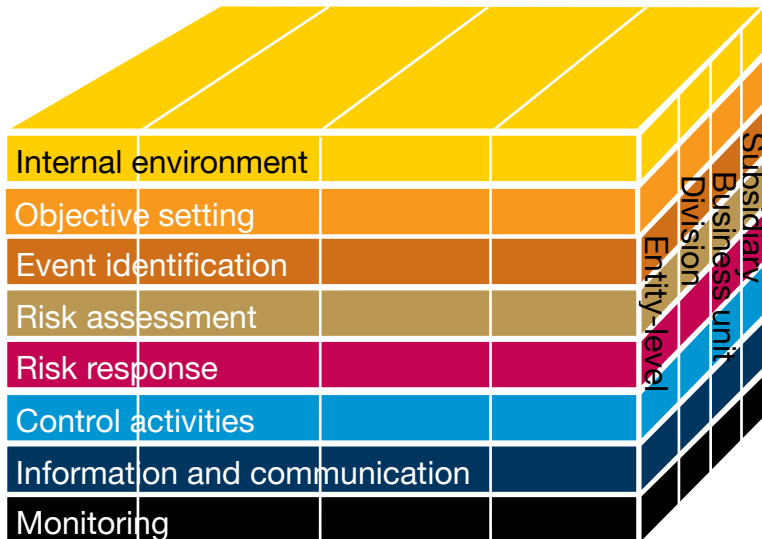
- Monitoring – The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

Enterprise risk management is not strictly a serial process, where one component affects only the next. It is a multidirectional, iterative process in which almost any component can and does influence another.

Relationship of objectives and components

There is a direct relationship between objectives, which are what an entity strives to achieve, and enterprise risk management components, which represent what is needed to achieve them. The relationship is depicted in a three-dimensional matrix, in the form of a cube.

The four objectives categories – strategic, operations, reporting, and compliance – are represented by the vertical columns, the eight components by horizontal rows, and an entity’s units by the third dimension. This depiction portrays the ability to focus on the entirety of an entity’s enterprise risk management, or by objectives category, component, entity unit, or any subset thereof.



Effectiveness

Determining whether an entity’s enterprise risk management is “effective” is a judgment resulting from an assessment of whether the eight components are present and functioning effectively. Thus, the components are also criteria for effective enterprise risk management. For the components to be present and functioning properly there can be no material weaknesses, and risk needs to have been brought within the entity’s risk appetite.

When enterprise risk management is determined to be effective in each of the four categories of objectives, respectively, the board of directors and management have reasonable assurance that they understand the extent to which the entity’s strategic and operations objectives are being achieved, and that the entity’s reporting is reliable and applicable laws and regulations are being complied with.

The eight components will not function identically in every entity. Application in small and mid-size entities, for example, may be less formal and less structured. Nonetheless, small entities still can have effective enterprise risk management, as long as each of the components is present and functioning properly.

Limitations

While enterprise risk management provides important benefits, limitations exist. In addition to factors discussed above, limitations result from the realities that human judgment in decision making can be faulty, decisions on responding to risk and establishing controls need to consider the relative costs and benefits, breakdowns can occur because of human failures such as simple errors or mistakes, controls can be circumvented by collusion of two or more people, and management has the ability to override enterprise risk management decisions. These limitations preclude a board and management from having absolute assurance as to achievement of the entity's objectives.

Encompasses internal control

Internal control is an integral part of enterprise risk management. This enterprise risk management framework encompasses internal control, forming a more robust conceptualization and tool for management. Internal control is defined and described in *Internal Control – Integrated Framework*. Because that framework has stood the test of time and is the basis for existing rules, regulations, and laws, that document remains in place as the definition of and framework for internal control. While only portions of the text of *Internal Control – Integrated Framework* are reproduced in this framework, the entirety of that framework is incorporated by reference into this one.

Roles and responsibilities

Everyone in an entity has some responsibility for enterprise risk management. The chief executive officer is ultimately responsible and should assume ownership. Other managers support the entity's risk management philosophy, promote compliance with its risk appetite, and manage risks within their spheres of responsibility consistent with risk tolerances. A risk officer, financial officer, internal auditor, and others usually have key support responsibilities. Other entity personnel are responsible for executing enterprise risk management in accordance with established directives and protocols. The board of directors provides important oversight to enterprise risk management, and is aware of and concurs with the entity's risk appetite. A number of external parties, such as customers, vendors, business partners, external auditors, regulators, and financial analysts often provide information useful in effecting enterprise risk management, but they are not responsible for the effectiveness of, nor are they a part of, the entity's enterprise risk management.

Organization of this report

This report is in two volumes. The first volume contains the *Framework* as well as this *Executive Summary*. The *Framework* defines enterprise risk management and describes principles and concepts, providing direction

for all levels of management in businesses and other organizations to use in evaluating and enhancing the effectiveness of enterprise risk management. This *Executive Summary* is a high-level overview directed to chief executives, other senior executives, board members, and regulators. The second volume, *Application Techniques*, provides illustrations of techniques useful in applying elements of the framework.

Use of this report

Suggested actions that might be taken as a result of this report depend on position and role of the parties involved:

- **Board of Directors** – The board should discuss with senior management the state of the entity’s enterprise risk management and provide oversight as needed. The board should ensure it is apprised of the most significant risks, along with actions management is taking and how it is ensuring effective enterprise risk management. The board should consider seeking input from internal auditors, external auditors, and others.
- **Senior Management** – This study suggests that the chief executive assess the organization’s enterprise risk management capabilities. In one approach, the chief executive brings together business unit heads and key functional staff to discuss an initial assessment of enterprise risk management capabilities and effectiveness. Whatever its form, an initial assessment should determine whether there is a need for, and how to proceed with, a broader, more in-depth evaluation.
- **Other Entity Personnel** – Managers and other personnel should consider how they are conducting their responsibilities in light of this framework and discuss with more senior personnel ideas for strengthening enterprise risk management. Internal auditors should consider the breadth of their focus on enterprise risk management.
- **Regulators** – This framework can promote a shared view of enterprise risk management, including what it can do and its limitations. Regulators may refer to this framework in establishing expectations, whether by rule or guidance or in conducting examinations, for entities they oversee.
- **Professional Organizations** – Rule-making and other professional organizations providing guidance on financial management, auditing, and related topics should consider their standards and guidance in light of this framework. To the extent diversity in concepts and terminology is eliminated, all parties benefit.
- **Educators** – This framework might be the subject of academic research and analysis, to see where future enhancements can be made. With the presumption that this report becomes accepted as a common ground for understanding, its concepts and terms should find their way into university curricula.

With this foundation for mutual understanding, all parties will be able to speak a common language and communicate more effectively. Business executives will be positioned to assess their company’s enterprise risk management process against a standard, and strengthen the process and move their enterprise toward established goals. Future research can be leveraged off an established base. Legislators and regulators will be able to gain an increased understanding of enterprise risk management, including its benefits and limitations. With all parties utilizing a common enterprise risk management framework, these benefits will be realized.

Contacts

Rossana S. Javier
Managing Partner
rose.javier@ph.pwc.com
+63 (2) 459 3016

Nerissa R. Mendoza
Executive Director
neri.mendoza@ph.pwc.com
+63 (2) 459 3094

April Theresa D.C. Bernardino
Executive Director
april.c.bernardino@ph.pwc.com
+63 (2) 459 3095

Michelle F. Tengonciang
Director
michelle.a.fajardo@ph.pwc.com
+63 (2) 459 3097

Roberto C. Bassig
Director
robert.bassig@ph.pwc.com
+63 (2) 459 3142

pwc.com

