COSO

Committee of Sponsoring Organizations of the Treadway Commission

Internal Control—Integrated Framework

Framework and Appendices

September 2012

Post Public Exposure Version

To submit comments on this Public Exposure Draft, please visit the **www.ic.coso.org** website. Responses are due by November 16, 2012.

Respondents will be asked to respond to a series of questions. Those questions may be found on-line at **www.ic.coso.org** and in a separate document provided at the time of download. Respondents may upload letters through this site. Please do not send responses by fax.

Written comments on this exposure draft will become part of the public record and will be available on-line March 31, 2013.

Post Public Exposure Version

Internal Control—Integrated Framework

Framework and Appendices

September 2012

Committee of Sponsoring Organizations of the Treadway Commission

To submit comments on this Public Exposure Draft, please visit the **www.ic.coso.org** website. Responses are due by November 16, 2012.

Respondents will be asked to respond to a series of questions. Those questions may be found on-line at **www.ic.coso.org** and in a separate document provided at the time of download. Respondents may upload letters through this site. Please do not send responses by fax.

Written comments on this exposure draft will become part of the public record and will be available on-line March 31, 2013.

Committee of Sponsoring Organizations of the Treadway Commission

Board Members	*Representative*
COSO Chair	David L. Landsittel
American Accounting Association	Mark S. Beasley Douglas F. Prawitt
The Institute of Internal Auditors	Richard F. Chambers
American Institute of Certified Public Accountants	Charles E. Landes
Financial Executives International	Marie N. Hollein
Institute of Management Accountants	Sandra Rictermeyer Jeffrey C. Thomson

PwC
Author

Principal Contributors

Miles E.A. Everson	Engagement Leader	New York, USA
Stephen E. Soske	Project Lead Partner	Boston, USA
Frank J. Martens	Project Lead Director	Vancouver, Canada
Cara M. Beston	Partner	San Jose, USA
Charles E. Harris	Partner	Florham Park, USA
J. Aaron Garcia	Director	San Diego, USA
Catherine I. Jourdan	Director	Paris, France
Jay A. Posklensky	Director	Florham Park, USA
Sallie Jo Perraglia	Manager	New York, USA

Advisory Council

Sponsoring Organizations Representatives

Audrey A. Gramling	Bellarmine University	Fr. Raymond J. Treece Endowed Chair
Steven E. Jameson	Community Trust Bank	Executive Vice President and Chief Internal Audit & Risk Officer
J. Stephen McNally	Campbell Soup Company	Finance Director/Controller
Ray Purcell	Pfizer	Director of Financial Controls
Bill Schneider	AT&T	Director of Accounting

Members at Large

Jennifer Burns	Deloitte	Partner
Jim DeLoach	Protiviti	Managing Director
Trent Gazzaway	Grant Thornton	Partner
Cees Klumper	The Global Fund to Fight AIDS, Tuberculosis and Malaria	Chief Risk Officer
Thomas Montminy	PwC	Partner
Al Paulus	E&Y	Partner
Thomas Ray	KPMG	Partner
Dr. Larry E. Rittenberg	University of Wisconsin	Emeritus Professor of Accounting Chair Emeritus COSO
Ken Vander Wal	ISACA	President

Regulatory Observers and Other Observers

James Dalkin	Government Accountability Office	Director in the Financial Management and Assurance Team
Harrison E. Greene, Jr.	Federal Deposit Insurance Corporation	Assistant Chief Accountant
Christian Peo	Securities and Exchange Commission	Professional Accounting Fellow (Through June 2012)
Amy Steele	Securities and Exchange Commission	Associate Chief Accountant (Commencing July 2012)
Vincent Tophoff	International Federation of Accountants	Senior Technical Manager
Keith Wilson	Public Company Accounting Oversight Board	Deputy Chief Auditor

Additional PwC Contributors

Joseph Atkinson	Partner	New York, USA
Jeffrey Boyle	Partner	Tokyo, Japan
Glenn Brady	Partner	St. Louis, USA
James Chang	Partner	Beijing, China
Mark Cohen	Partner	San Francisco, USA
Andrew Dahle	Partner	Chicago, USA
Megan Haas	Partner	Hong Kong, China
Junya Hakoda	Partner (Retired)	Tokyo, Japan
Diana Hillier	Partner	London, England
Steve Hirt	Partner	Boston, USA
Brian Kinman	Partner	St. Louis, USA
Barbara Kipp	Partner	Boston, USA
Hans Koopmans	Partner	Singapore
Sachin Mandal	Partner	Florham Park, USA
Alan Martin	Partner	Frankfurt, Germany
Pat McNamee	Partner	Florham Park, USA
Jonathan Mullins	Partner (Retired)	Dallas, USA
Simon Perry	Partner	London, England
Andrew Reinsel	Partner	Cincinnati, USA
Kristin Rivera	Partner	San Francisco, USA
Valerie Wieman	Partner	Florham Park, USA
Alexander Young	Partner	Toronto, Canada
David Albright	Principal	Washington, D.C., USA
Charles Yovino	Principal	Atlanta, USA
Eric M. Bloesch	Managing Director	Philadelphia, USA
Christopher Michaelson	Director	Minneapolis, USA
Lisa Reshaur	Director	Seattle, USA
Tracy Walker	Director	Bangkok, Thailand
Qiao Pan	Senior Associate	New York, USA

Preface

This project was commissioned by COSO, which is dedicated to providing thought leadership through the development of comprehensive frameworks and guidance on internal control, enterprise risk management, and fraud deterrence designed to improve organizational performance and oversight and to reduce the extent of fraud in organizations. COSO is a private sector initiative, jointly sponsored and funded by:

- American Accounting Association (AAA)
- American Institute of Certified Public Accountants (AICPA)
- Financial Executives International (FEI)
- Institute of Management Accountants (IMA)
- The Institute of Internal Auditors (IIA)

Post Public Exposure Version

Table of Contents

Foreword

1 In 1992 the Committee of Sponsoring Organizations of the Treadway Commission (COSO) released its *Internal Control—Integrated Framework* (the original framework). The original framework has gained broad acceptance and is widely used around the world. It is recognized as a leading framework for designing, implementing, and conducting internal control and assessing the effectiveness of internal control.

2 In the twenty years since the inception of the original framework, business and operating environments have changed dramatically, becoming increasingly complex, technologically driven, and global. At the same time, stakeholders are more engaged, seeking greater transparency and accountability for the integrity of systems of internal control that support business decisions and governance of the organization.

3 COSO is pleased to present the updated Internal Control—Integrated Framework (Framework). COSO believes the Framework will enable organizations to effectively and efficiently develop and maintain systems of internal control that can enhance the likelihood of achieving the entity's objectives and adapt to changes in the business and operating environments.

4 The experienced reader will find much that is familiar in the Framework, which builds on what has proven useful in the original version. It retains the core definition of internal control and the five components of internal control. The requirement to consider the five components to assess the effectiveness of a system of internal control remains fundamentally unchanged. Also, the Framework continues to emphasize the importance of management judgment in designing, implementing, and conducting internal control, and in assessing the effectiveness of a system of internal control.

5 At the same time, the Framework includes enhancements and clarifications that are intended to ease use and application. One of the more significant enhancements is the formalization of fundamental concepts introduced in the original framework as principles. These principles, associated with the five components, provide clarity for the user in designing and implementing systems of internal control and for understanding requirements for effective internal control.

6 The Framework has been enhanced by expanding the financial reporting category of objectives to include other important forms of reporting, such as non-financial and internal reporting. Also, the Framework reflects considerations of many changes in the business, operating, and regulatory environments over the past several decades, including:

- Expectations for governance oversight
- Globalization of markets and operations
- Changes and greater complexity in the business
- Demands and complexities in laws, rules, regulations, and standards
- Expectations for competencies and accountabilities
- Use of, and reliance on, evolving technologies
- Expectations relating to preventing and detecting fraud

7 COSO is pleased to present the Framework in three volumes. The first is an *Executive Summary*: a high-level overview intended for the board of directors, chief executive officer, other senior management, regulators, and standard setters. The second volume, *Framework and Appendices*, sets out the Framework, including the definition of internal control and the components and principles supporting effective systems of internal control. Included within the Framework are the following chapters:

- Definition of Internal Control
- Objectives, Components, and Principles
- Effective Internal Control
- Additional Considerations
- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring Activities
- Limitations

8 The second volume provides direction for all levels of management to use in designing, implementing, and conducting internal control and assessing its effectiveness. The appendices to the second volume provide reference, but are not considered a part of the Framework. The third volume, *Illustrative Tools for Assessing Effectiveness of a System of Internal Control*, provides templates and scenarios that may be useful in applying the Framework.

9 In addition to the three volumes, *Internal Control over External Financial Reporting: Compendium of Approaches and Examples* has been published concurrently to provide practical approaches and examples that illustrate how the components and principles set forth in the Framework can be applied in preparing external financial statements.

10 COSO may, in the future, issue other documents to provide assistance in applying the Framework. However, neither the *Internal Control over External Financial Reporting: Compendium of Approaches and Examples* nor any other future guidance takes precedence over the Framework.

11 Among other publications published by COSO is the *Enterprise Risk Management—Integrated Framework* (the *ERM Framework*). The *ERM Framework* and the Framework are intended to be complementary, and neither supersedes the other. Yet, while these frameworks are distinct and provide a different focus, they do overlap. The *ERM Framework* encompasses internal control, with several portions of the text of the original *Internal Control—Integrated Framework* reproduced. Consequently, the *ERM Framework* remains a viable and suitable framework for designing, implementing, conducting, and assessing enterprise risk management. Organizations that have implemented the *ERM Framework* will likely see minimal impact on their enterprise risk management efforts resulting from the issuance of this updated version of *Internal Control—Integrated Framework: Framework and Appendices*.

12 Finally, the COSO Board would like to thank PwC and the Advisory Council for their contributions in developing the Framework and related documents. Their full consideration of input provided by many stakeholders and their attention to detail were instrumental in ensuring that the core strengths of the original framework have been preserved, clarified, and strengthened.

1. Definition of Internal Control

13 The purpose of this Internal Control—Integrated Framework (Framework) is to help management better control the organization and to provide a board of directors[1] with an added ability to oversee internal control. A system of internal control allows management to stay focused on the organization's pursuit of its operations and financial performance goals, while operating within the confines of relevant laws and minimizing surprises along the way. Internal control enables an organization to deal more effectively with changing economic and competitive environments, leadership, priorities, and evolving business models.

Understanding Internal Control

14 Internal control is defined as follows:

> *Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.*

15 This definition emphasizes that internal control is:

- *Geared to the achievement of objectives* in one or more separate but overlapping categories
- *A process* consisting of ongoing tasks and activities—it is a means to an end, not an end in itself
- *Effected by people*—it is not merely about policy and procedure manuals, systems, and forms, but about people and the actions they take at every level of an organization to effect internal control
- Able to *provide reasonable assurance*, not absolute assurance, to an entity's senior management and board of directors
- *Adaptable to the entity structure*—flexible in application for the entire entity or for a particular subsidiary, division, operating unit, or business process

16 This definition of internal control is intentionally broad for two reasons. First, it captures important concepts that are fundamental to how organizations design, implement, and conduct internal control and assess effectiveness of their system of internal control, providing a basis for application across various types of organizations, industries, and geographic regions. Second, the definition accommodates subsets of internal control.

17 Those who want to may focus separately, for example, on internal control over reporting or controls relating to complying with laws and regulations. Similarly, a directed focus on controls in particular units or activities of an entity can be accommodated.

1 The Framework uses the term "board of directors," which encompasses the governing body, including board, board of trustees, general partners, owner, or supervisory board.

18 It also provides flexibility in application, allowing an organization to sustain internal control across the entire entity; at a subsidiary, division, or operating unit level; or within a function relevant to the entity's operations, reporting, or compliance objectives, based on the entity's specific needs or circumstances.

Geared to the Achievement of Objectives

19 The Framework sets forth three categories of objectives, which allow organizations to focus on separate aspects of internal control:

- *Operations Objectives*—These pertain to effectiveness and efficiency of the entity's operations, including operational and financial performance goals, and safeguarding assets against loss.
- *Reporting Objectives*—These pertain to internal and external financial and non-financial reporting and may encompass reliability, timeliness, transparency, or other terms as set forth by regulators, standard setters, or the entity's policies.
- *Compliance Objectives*—These pertain to adherence to laws and regulations to which the entity is subject.

20 These distinct but overlapping categories—a particular objective can fall under more than one category—address different needs and may be the direct responsibility of different individuals. The three categories also indicate what can be expected from internal control.

21 A system of internal control is expected to provide an organization with reasonable assurance that those objectives relating to external reporting and compliance with laws and regulations will be achieved. Achieving those objectives, which are based largely on laws, rules, regulations, or standards established by legislators, regulators, and standard setters, depends on how activities within the organization's control are performed. Generally, management and/or the board have greater discretion in setting internal reporting objectives that are not driven primarily by such external parties. However, the organization may choose to align its internal and external reporting objectives to allow internal reporting to better support the entity's external reporting.

22 In those instances where the organization operates in accordance with external standards—for instance in applying an external standard relating to quality or information processing—an organization is able to attain reasonable assurance that objectives relating to the efficiency and effectiveness of operations are achieved. However, achievement of operations objectives—such as a particular return on investment, market share, or entry into new product lines—is not always within the organization's control. Internal control cannot prevent bad judgments or decisions, or external events that can cause an organization to fail to achieve operational goals. For these objectives, systems of internal control can only provide reasonable assurance that management and the board are made aware, in a timely manner, of the extent to which the entity is moving toward those objectives.

A Process

23 Internal control is not one event or circumstance, but a dynamic and iterative process[2]—actions that permeate an entity's activities and that are inherent in the way management runs the entity. Embedded within this process are controls consisting of policies and procedures. These policies reflect management or board statements of what should be done to effect internal control. Such statements may be documented, explicitly stated in other management communications, or implied through management actions and decisions. Procedures consist of actions that implement a policy.

24 Business processes, which are conducted within or across operating units or functional areas, are managed through the fundamental management activities, such as planning, executing, and checking. Internal control is integrated with these processes. Internal control embedded within these processes and activities are likely more effective and efficient.

Effected by People

25 Internal control is effected by the board of directors, management, and other personnel. It is accomplished by the people of an organization, by what they do and say. People establish the entity's objectives and put actions in place to achieve specified objectives.

26 The board's oversight responsibilities include providing advice and direction to management, constructively challenging management, approving policies and transactions, and monitoring management's activities. Consequently, the board of directors is an important element of internal control. The board and senior management establish the tone for the organization concerning the importance of internal control and the expected standards of conduct across the entity.

27 Issues arise every day in managing an entity. People may not fully understand the nature of such issues or alternatives available to them, communicate effectively, or perform consistently. Each individual brings to the workplace a unique background and ability, and each has different needs and priorities. These individual differences can be inherently valuable and beneficial to innovation and productivity, but if not properly aligned with the entity's objectives they can be counterproductive. Yet, people must know their responsibilities and limits of authority. Accordingly, a clear and close linkage needs to exist between people's roles and responsibilities and the way in which these duties are carried out and aligned with the entity's objectives.

Provides Reasonable Assurance

28 An effective system of internal control provides management and the board of directors with reasonable assurance regarding achievement of an entity's objectives. The term "reasonable assurance" rather than "absolute assurance" acknowledges that limitations exist in all systems of internal control, and that uncertainties and risks may exist, which no one can confidently predict with precision. Absolute assurance is not possible.

2 Although referred to as a process, internal control comprises many processes.

29 Reasonable assurance does not imply that an entity will always achieve its objectives. Effective internal control increases the likelihood of an entity achieving its objectives. However, the likelihood of achievement is affected by limitations inherent in all internal control systems, such as human error and the uncertainty inherent in judgment. Additionally, a system of internal control can be circumvented if people collude. Further, if management is able to override controls, the entire system may fail. In other words, even an effective system of internal control can experience a failure.

Adaptable to the Entity Structure

30 Entities may be structured along various dimensions. The management operating model may follow product or service lines; reporting may be done for a consolidated entity, division, or operating unit, with geographic markets providing for further subdivisions or aggregations of performance. The management operating model may utilize outsourced service providers to support the achievement of objectives.

31 The legal entity structure is typically designed to follow regulatory reporting requirements, limit risk, or provide tax benefits. Often the organization of legal entities is quite different from the management operating model used to manage operations, allocate resources, measure performance, and report results.

32 Internal control can be applied, based on management's decision and in the context of legal or regulatory requirements, to the management operating model, legal entity structure, or a combination of these.

2. Objectives, Components, and Principles

Introduction

33 An organization adopts a mission and vision, sets strategies, establishes objectives it wants to achieve, and formulates plans for achieving them. Objectives may be set for an entity as a whole, or be targeted to specific activities within the entity. Though many objectives are specific to a particular entity, some are widely shared. For example, objectives common to most entities are sustaining organizational success, reporting to stakeholders, recruiting and retaining motivated and competent employees, achieving and maintaining a positive reputation, and complying with laws and regulations.

34 Supporting the organization in its efforts to achieve objectives are five components of internal control:

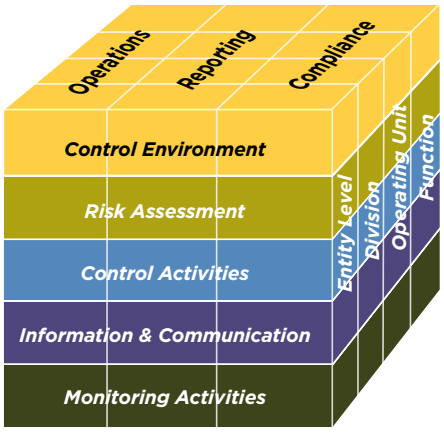
- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring Activities

35 These components are relevant to an entire entity and to the entity level, its subsidiaries, division, or any of its individual operating units, functions, or other subsets of the entity.

Relationship of Objectives, Components, and the Entity

36 A direct relationship exists between objectives, which are what an entity strives to achieve, components, which represent what is required to achieve the objectives, and entity structure (the operating units, legal entities, and other structures). The relationship can be depicted in the form of a cube.

- The three categories of objectives are represented by the columns.
- The five components are represented by the rows.
- The entity structure, which represents the overall entity, divisions, subsidiaries, operating units, or functions, including business processes such as sales, purchasing, production, and marketing and to which internal control relates, are depicted by the third dimension of the cube.[3]



3 Throughout the Framework, the term "the entity and its subunits" refers collectively to the overall entity, divisions, subsidiaries, operating units, and functions.

37 Each component cuts across and applies to all three categories of objectives. For example, selecting policies and procedures that help ensure that management's statements, actions, and decisions are carried out—part of the control activities component—are relevant to all three objectives categories.

38 The three categories of objectives are not parts or units of the entity. For instance, operations objectives relate to the efficiency and effectiveness of operations, not specific operating units or functions such as sales, marketing, procurement, or human resources.

39 Accordingly, when considering the category of objectives related to reporting, for example, knowledge of a wide array of information about the entity's operations is needed. In that case, focus is on the middle column of the model—reporting objectives—rather than the operations objectives category.

40 Internal control is a dynamic, iterative, and integrated process. For example, risk assessment not only influences the control environment and control activities, but also may highlight a need to reconsider the entity's requirements for information and communication, or for its monitoring activities. Thus, internal control is not a linear process where one component affects only the next. It is an integrated process in which components can and will impact another.

41 No two entities will, or should, have the same system of internal control. Entities, objectives, and systems of internal control differ dramatically by industry and regulatory environment, as well as by internal considerations such as the size, nature of the management operating model, tolerance for risk, reliance on technology, and competence and number of personnel. Thus, while all entities require each of the components to maintain effective internal control over their activities, one entity's system of internal control usually looks different from another's.

Objectives

42 Management, with board oversight, sets entity-level objectives that align with the entity's mission, vision, and strategies. These high-level objectives reflect choices made by management and board of directors about how the organization seeks to create, preserve, and realize value for its stakeholders. Such objectives may focus on the entity's unique operations needs, or align with laws, rules, regulations, and standards imposed by legislators, regulators, and standard setters, or some combination of the two. Setting objectives is a prerequisite to internal control and a key part of the management process relating to strategic planning.

43 Individuals who are part of the system of internal control need to understand the overall strategies and objectives set by the organization. As part of internal control, management specifies suitable objectives so that risks to the achievement of such objectives can be identified and assessed. Specifying objectives relates to the articulation of specific, measurable or observable, attainable, relevant, and time-bound objectives.

44 In most instances, specifying objectives requires some form of codification. However there may be instances where an entity might not explicitly state an objective. Objectives specified in appropriate detail can be readily understood by the people who are working toward achieving them.

Categories of Objectives

45 The Framework groups entity objectives into the three categories of operations, reporting, and compliance.

Operations Objectives

46 Operations objectives relate to the achievement of an entity's basic mission and vision—the fundamental reason for its existence. These objectives vary based on management's choices relating to the management operating model, industry considerations, and performance. Entity-level objectives cascade into related sub-objectives for operations within divisions, subsidiaries, operating units, and functions, directed at enhancing effectiveness and efficiency in moving the entity toward its ultimate goal.

47 As such, operations objectives may relate to improving financial performance, productivity (e.g., avoiding waste and rework), quality, environmental practices, innovation, and customer and employee satisfaction. These objectives pertain to all types of entities. For example, a for-profit entity may focus on revenue, profitability, return on assets, and liquidity. In contrast, a not-for-profit entity, though certainly concerned with revenues or levels of spending, may focus more on increasing donor participation. A governmental agency may focus primarily on executing its spending in line with the designated purposes of its appropriators to ensure that the spending supports its mission objectives. If an entity's operations objectives are not well conceived or clearly specified, its resources may be misdirected.

Safeguarding of Assets

48 The operations category of objectives includes safeguarding of assets, which refers to protecting and preserving entity assets. For instance, an entity may set objectives relating to the prevention of loss of assets and the timely detection and reporting of any such losses. These objectives form the basis of assessing risk relating to safeguarding of assets and selecting and developing controls needed to mitigate such risk.

49 The efficient use of an entity's assets, and prevention of loss through waste, inefficiency, or poor business decisions (e.g., selling product at too low a price, extending credit to bad risks, failing to retain key employees, preventing patent infringement, incurring unforeseen liabilities) relate to a broader operations objectives and are not a specific consideration relating to safeguarding of assets.

50 Laws, rules, regulations, and standards have created an expectation that management reporting on internal control includes controls relating to preventing and detecting unauthorized acquisition, use, or disposition of the assets. In addition, some entities consider safeguarding of assets a separate category of objective, and that view can be accommodated within the application of the Framework.

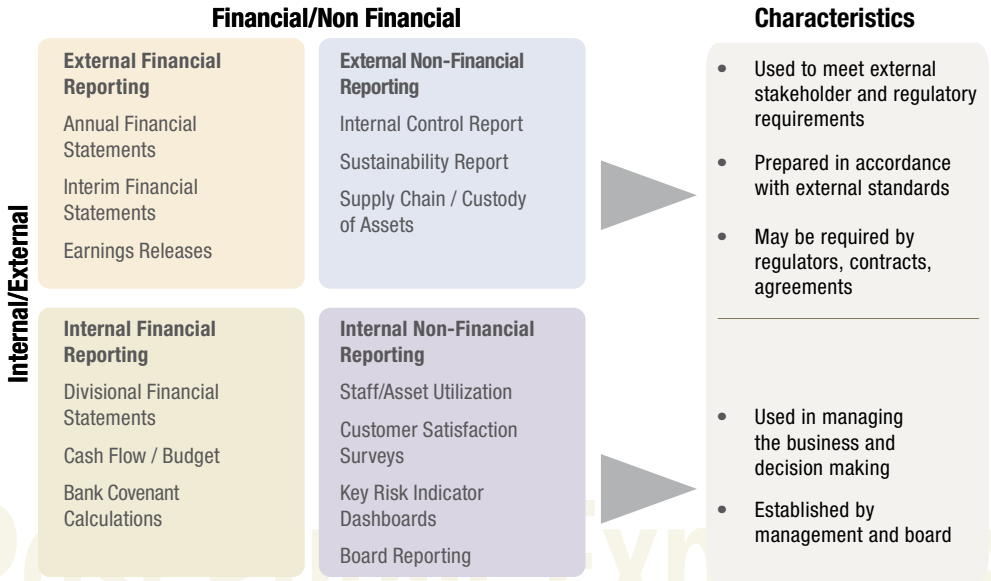
Reporting Objectives

51 Reporting objectives pertain to the preparation of reports for use by organizations and stakeholders. Reporting objectives may relate to financial or non-financial reporting and to internal or external reporting. Internal reporting objectives are driven by internal requirements in response to a variety of potential needs such as the entity's strategic directions, operating plans, and performance metrics at various levels. External reporting objectives are driven primarily by regulations and/or standards established by regulators, and standard-setting bodies.

- *External Financial Reporting Objectives*—Entities need to achieve external financial reporting objectives to meet obligations to and expectations of stakeholders. Financial statements are necessary for accessing capital markets and may be critical to being awarded contracts or in dealing with suppliers and vendors. Investors, analysts, and creditors often rely on an entity's external financial statements to assess its performance against peers and alternative investments. Management may also be required to publish financial statements using objectives set forth by rules, regulations, and standards.
- *External Non-Financial Reporting Objectives*—Management may report external non-financial information in accordance with regulations, standards, or frameworks. An entity may engage an independent auditor to report on its conformance with standards published by standard-setting bodies. Non-financial reporting requirements as set forth by regulations and standards for management reporting on the effectiveness of internal control over financial reporting are part of external non-financial reporting objectives. For purposes of the Framework, external reporting in the absence of a regulation, standard, or framework represents external communication.
- *Internal Financial and Non-Financial Reporting Objectives*—Internal reporting to management and the board of directors includes information deemed necessary to manage the organization. It supports decision making and assessment of the entity's activities and performance. Internal reporting objectives are based on preferences and judgments of management and the board. Internal reporting objectives vary among entities because different organizations have different strategic directions, operating plans, and expectations.

Relationship within Reporting Category of Objectives

52 The overall relationship between the four sub-categories of reporting objectives is shown in the graphic below.



53 Reporting objectives are different from the information and communication component of internal control. Management establishes, with board oversight, reporting objectives when the organization needs reasonable assurance of achieving a particular reporting objective. In these situations all five components of internal control are needed. For instance, in preparing internal non-financial reporting to the board on the status of merger integration efforts, the organization specifies the reporting objectives (e.g., prepares reliable, relevant, and useful reports), assigns competent individuals, assesses risks relating to specified objectives, selects and develops controls within the five components necessary to mitigate such risks, and monitors components of internal control supporting the specified non-financial reporting objective.

54 In contrast, the Information and Communication component supports the functioning of all components of objectives, as well as operations and compliance objectives. For instance, controls within information and communication supports the preparation of the above report, helping to provide relevant and quality information underlying the report, but these controls are only part of the overall system of internal control.

Compliance Objectives

55 Entities must conduct activities, and often take specific actions, in accordance with applicable laws and regulations. As part of specifying compliance objectives, the organization needs to understand which laws and regulations apply across the entity. Many laws and regulations are generally well known, such as those relating to taxation and environmental compliance, but others may be more obscure, such as those that apply to an entity conducting operations in a remote foreign territory.

56 Laws and regulations establish minimum standards of conduct expected of the entity. The organization is expected to incorporate these standards into the objectives set for the entity. Some organizations will set objectives to a higher level of performance than established by laws and regulations. In setting those objectives, management is able to exercise discretion relative to the performance of the entity. For instance, a particular law may limit minors working outside school hours to eighteen hours in a school week. However, a retail food service company may choose to limit its minor-age staff to working fifteen hours per week.

57 For purposes of the Framework, compliance with an entity's internal policies and procedures, as opposed to compliance with external laws and regulations as discussed above, relates to operations objectives.

Overlap of Objectives Categories

58 An objective in one category may overlap or support an objective in another. For example, "closing financial reporting period within five workdays" may be a goal supporting primarily an operations objective—to support management in reviewing business performance. But it also supports timely reporting and filings with regulatory agencies.

59 The category in which an objective falls may vary depending on the circumstances. For instance, controls to prevent theft of assets—such as maintaining a fence around inventory, or having a gatekeeper to verify proper authorization of requests for movement of goods—fall under the operations category. These controls may not be relevant to reporting where inventory losses are detected after a periodic physical inspection and recording in the financial statements. However, if for reporting purposes management relies solely on perpetual inventory records, as may be the case for interim or internal financial reporting, the physical security controls would then also fall within the reporting category. These physical security controls, along with controls over the perpetual inventory records, are needed to achieve reporting objectives. A clear understanding is needed of the entity's business processes, policies and procedures, and the respective impact on each category of objectives.

Basis of Objectives Categories

60 Some objectives are derived from the regulatory or industry environments in which the entity operates. For example:

- Some entities submit information to environmental agencies.

- Publicly traded companies file information with securities regulators.
- Universities report grant expenditures to government agencies.

61 These objectives are established largely by law or regulation, and fall into the category of compliance, external reporting, or, in these examples, both.

62 Conversely, operations and internal reporting objectives are based more on the organization's preferences, judgments, and choices. These objectives vary widely among entities simply because informed and competent people may select different objectives. For example, one organization might choose to be an early adopter of emerging technologies in developing new products, whereas another might be a quick follower, and yet another a late adopter. These choices would reflect the entity's strategies and the competencies, technologies, and controls within its research and development function. Consequently, no one formulation of objectives can be optimal for all entities.

Objectives and Sub-Objectives

63 Management links specified entity-level objectives to more specific sub-objectives that cascade throughout the organization. Sub-objectives also are established as part of or flowing from the strategy-setting process, and relate to the entity and its subunits and functional activities such as sales, production, engineering, marketing, productivity, employee engagement, innovation, and information technology. Management aligns these sub-objectives with entity-level objectives and coordinates these across the entity.

64 Where entity-level objectives are consistent with prior practice and performance, the linkage between activities is usually known. Where objectives depart from an entity's past practices, management addresses the linkages or accepts increased risks. For example, an entity-level objective relating to customer satisfaction depends on linked sub-objectives dealing with the introduction of services that use a newer and less proven technology infrastructure. These sub-objectives might need to be substantially changed if past practice used older, proven technologies.

65 Sub-objectives for operating units and functional activities also need to be specific, measurable or observable, attainable, relevant, and time-bound. In addition, they must be readily understood by the people who are working toward achieving them. Management and other personnel require a mutual understanding of both what is to be accomplished and the means of determining to what extent it is accomplished in order to ensure individual and team accountability.

66 Entities specify multiple sub-objectives for each activity, flowing both from the entity-level objectives and from established standards relating to compliance and reporting objectives, as deemed suitable in the circumstances. For example, procurement operations objectives may be to:

- Purchase goods that meet engineering specifications
- Purchase goods from companies that meet environmental, health, and safety specifications (e.g., no child labor, good working conditions)

- Negotiate acceptable prices and other terms

67 As another example, when specifying suitable external reporting objectives relating to the preparation of external financial statements, Objectives, Components, and Principles 12 management considers accounting standards, financial statement assertions, and qualitative characteristics that are applicable to the entity and its subunits. For example, management may set an entity-level external financial reporting objective as follows: "Our company prepares reliable financial statements reflecting activities in accordance with generally accepted accounting principles."

68 Management also specifies suitable sub-objectives for divisions, subsidiaries, operating units, and functions with sufficient clarity to support entity-level objectives. For instance, management specifies subobjectives for sales transactions that apply applicable accounting standards based on the circumstances and that address relevant financial statement assertions and qualitative characteristics, such as:

- All sales transactions that occur are recorded on a timely basis.
- Sales transactions are recorded at correct amounts in the right accounts.
- Sales transactions are accurately and completely summarized in the entity's books and records.
- Presentation and disclosures relating to sales are properly described, sorted, and classified.

Components and Principles of Internal Control

69 The Framework sets out five components of internal control and seventeen principles representing the fundamental concepts associated with components. These components and principles of internal control are suitable for all entities. All seventeen principles apply to each category of objective, as well as to objectives and sub-objectives within a category. For instance, an entity may apply the Framework relative to complying with a specific law regarding commercial arrangements with foreign entities, a subcategory of the compliance category of objectives.

70 Below is a summary of each of the five components of internal control and the principles relating to components. Each of the principles is covered in the respective component chapters.[4]

Control Environment

71 The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The board of directors and senior management establish the tone at the top regarding the importance of internal control and expected standards of conduct.

4 For purposes of the Framework, when describing principles the term "organization" is used to capture the meaning of, collectively, the board of directors, management, and other personnel. Typically the board of directors serves an oversight capacity within this term.

72 There are five principles relating to Control Environment:

1. The organization demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Risk Assessment

73 Risk assessment involves a dynamic and iterative process for identifying and analyzing risks to achieving the entity's objectives, forming a basis for determining how risks should be managed. Management considers possible changes in the external environment and within its own business model that may impede its ability to achieve its objectives.

There are four principles relating to Risk Assessment:

6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.
9. The organization identifies and assesses changes that could significantly impact the system of internal control.

Control Activities

74 Control activities are the actions established by policies and procedures to help ensure that management directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity and at various stages within business processes, and over the technology environment.

75 There are three principles relating to Control Activities:

10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
11. The organization selects and develops general control activities over technology to support the achievement of objectives.
12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Information and Communication

76 Information is necessary for the entity to carry out internal control responsibilities in support of achievement of its objectives. Communication occurs both internally and externally and provides the organization with the information needed to carry out day-to-day internal control activities. Communication enables personnel to understand internal control responsibilities and their importance to the achievement of objectives.

77 There are three principles relating to Information and Communication:

13. The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.
14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of other components of internal control.
15. The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.

Monitoring Activities

78 Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to effect the principles within each component, are present and functioning. Findings are evaluated and deficiencies are communicated in a timely manner, with serious matters reported to senior management and to the board.

79 There are two principles relating to Monitoring Activities:

16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Internal Control and the Management Process

80 Because internal control is a part of management's overall responsibility, the five components are discussed in the context of the management of the entity. Not every decision or action of management, however, is part of internal control:

- Having a board that comprises directors with sufficient independence from management and that carries out its oversight role is part of internal control. However, many decisions reached by the board are not part of internal control; for example approving a particular mission or vision. The board also fulfills a variety of governance responsibilities in addition to its responsibilities for oversight of internal control.
- Making strategic decisions impacting the entity's objectives is not part of internal control. An organization may apply enterprise risk management approaches or other approaches in setting objectives.
- Setting the overall level of acceptable risk and associated risk appetite[5] is part of strategic planning and enterprise risk management, not part of internal control. Similarly, setting risk tolerance levels in relation to specific objectives is also not part of internal control.
- Selecting and developing control activities designed to mitigate risks based on the organization's risk assessment process is a part of internal control; however, choosing which risk response is preferred to address specific risks is not part of internal control.

Internal Control and Objective-Setting

81 It is not practical to design and implement a system of internal control unless the entity's objectives are established, set, and specified for the organization. Establishing and setting objectives and related sub-objectives are parts of or flow from the strategic-planning process, with consideration given to laws, rules, regulations, and standards as well as management's own choices. However, internal control cannot dictate or establish what an entity's objectives should be.

82 As part of internal control, an organization specifies objectives by:

- Articulating and codifying specific, measurable or observable, attainable, relevant and time-based objectives
- Assessing suitability of objectives and sub-objectives for internal control based on facts, circumstances, and established laws, rules, regulations, and standards
- Communicating objectives and sub-objectives throughout the entity and sub-units

83 The following diagram illustrates establishing and setting objectives as part of the management process outside of internal control, and specifying and using objectives as part of internal control in the context of an external financial reporting and an operations objective.

5 "Risk appetite" is defined as the amount of risk, on a broad level, an entity is willing to accept in pursuit of its mission/vision.

Part of the Management Process		Part of Internal Control	
Establish ▶	Set ▶	Specify ▶	Use
External parties establish laws, rules, and standards (where applicable) relating to compliance and external financial reporting objectives.	Set strategic objectives and select strategy within the context of an entity's established mission or vision. Set entity-wide objectives and develop risk tolerances based on entity requirements. Align objectives with entity strategy and overall risk appetite. Set objectives and sub-objectives for the entity and its subunits.	Articulate specific, measurable or observable, attainable, relevant and time-based objectives. Assess suitablity of objectives and sub-objectives for internal control based on facts, circumstances, and established laws, rules, and standards. Communicate objectives and sub-objectives throughout the entity and its subunits.	Use specified objectives and sub-objectives as basis for risk assessment.
Examples of Financial Reporting Objectives and Sub-Objectives			
The Financial Accounting Standards Board (FASB) established accounting principles generally accepted in the United States of America (US GAAP).	Our company prepares reliable financial statements reflecting activities in accordance with US GAAP.	Management assesses whether US GAAP is relevant and appropriate in the circumstances. If not, management provides feedback to the objective-setting process.	Management identifies and assesses risk to preparing reliable financial statements reflecting activities in accordance with US GAAP.
A regulatory body establishes an accounting standard on revenue recognition.	Our company recognizes sales revenue upon installation of equipment for sales-type capital leases or recognizes rental revenue over the operating lease term.	Operating unit financial management assesses whether financial reporting objectives and sub-objectives relating to revenue recognition are relevant and appropriate to all equipment sales. If not, operating unit financial management provides feedback to the objective setting process.	Operating unit financial management identifies and assesses risk to recording revenue on equipment sales in accordance with US GAAP.
Example of Operations Objectives			
Not applicable for operations objectives.	Our company seeks to improve performance by increasing inventory turnover ratio to twelve times per year, recognizing that lower inventory levels may result in more backorder items for customers.	Operating unit management assesses whether operations objectives relating to inventory turnover goals are appropriate. If not, operating unit financial management provides feedback to the objective setting process.	Operating unit management identifies and assesses risk to the achievement of an inventory turnover ratio of twelve times per year.

Limitations of Internal Control

84 The Framework recognizes that while internal control provides reasonable assurance of achieving the entity's objectives, limitations do exist and may result from the:

- Suitability of objectives established as a precondition to internal control
- Reality that human judgment in decision making can be faulty
- Breakdowns that can occur because of human failures such as errors
- Ability of management to override internal control
- Ability of management, other personnel, and/or third parties to circumvent controls through collusion

85 These limitations preclude the board and management from having absolute assurance of the achievement of the entity's objectives—that is, internal control provides reasonable but not absolute assurance.

3. Effective Internal Control

Requirements for Effective Internal Control

86 An effective system of internal control provides reasonable assurance regarding achievement of an entity's objectives. Because internal control is relevant both to the entity and its subunits, an effective system of internal control may relate to a specific part of the organizational structure. An effective system of internal control reduces, to an acceptable level, the risk of not achieving an objective relating to one, two, or all three categories. It requires that:

- Each of the five components of internal control and relevant principles are present and functioning
- The five components are operating together in an integrated manner

87 When a major deficiency exists with respect to the presence and functioning of a component or relevant principle or in terms of the components operating together, the organization cannot conclude that it has met the requirements for an effective system of internal control.

88 When internal control is determined to be effective, senior management and the board of directors have reasonable assurance, that the organization:

- Achieves operations objectives when standards and criteria are established by legislators, regulators, and standard setters
- Understands the extent to which operations are managed effectively and efficiently when external standards do not exist
- Prepares reports in conformity with rules, regulations, and standards established by legislators, regulators, and standard setters, or with the entity's specified objectives and related policies
- Complies with applicable laws and regulations

89 The Framework sets forth that the components and relevant principles are requisite to an effective system of internal control. It does not prescribe the process for how management assesses its effectiveness.

Present and Functioning

90 The phrase "present and functioning" is applied to components and principles.

- "Present" refers to the determination that components and relevant principles exist in the design and implementation of the system of internal control.
- "Functioning" refers to the determination that components and relevant principles continue to exist in the operation and conduct of the system of internal control.

91 A component or relevant principle that is present and functioning implies that the organization:

- Understands the intent of components and how relevant principles are being applied
- Helps personnel understand and apply relevant principles across the entity
- Views weakness in, or absence of, a principle as a situation that triggers management attention

Role of Components

92 The Framework views all components of internal control as suitable and relevant to all entities, and therefore requires that all components be present and functioning and operating together in an integrated manner. Evaluating whether each component of internal control is present and functioning and whether the components are operating together requires consideration of how components are being applied by the entity within the system of internal control. Each of the five components operating together help to collectively reduce, to an acceptable level, the risk of not achieving an objective. When a component is deemed not to be present and functioning, or when components do not operate together, a major deficiency exists.

93 For instance, senior management determines whether the component of Information and Communication is operating together with the other components. Management asks the question, How does the organization use relevant, quality information (Information and Communication) in the component of Risk Assessment? Understanding how information is used (or not) is essential for determining whether these two components are operating together.

94 Other examples of components operating together include the following:

- An entity's commitment to employing competent resources reduces the risk of error in deploying control activities
- The board of directors' oversight of internal control reduces the risk of management override and fraud
- An entity's monitoring activities that evaluate and investigate unexpected results mitigate the risk of persistent errors in processing transactions

95 Components should not be viewed discretely; instead, they must operate together as an integrated system. However, in determining whether components operate together, the Framework does not allow management to determine that the presence and functioning of one component mitigates a major deficiency in another component.

96 Further, a change in one component should not be viewed in isolation. That is, management needs to assess the potential effects of a change in one component on other components.

97 Note that the notion that all five components of internal control must be present and functioning and operating together does not mean that each should function identically, or even at the same level, within an entity or in different entities. Effective systems of internal control can be designed, implemented, and conducted differently.

Role of Principles

98 Principles are fundamental concepts associated with components. As such, the Framework views the seventeen principles as suitable to all entities. Relevance refers to a determination that each principle has a significant bearing on the presence and functioning of its associated component.

99 The Framework presumes that principles are relevant. However, there may be a rare industry, operating, or regulatory situation in which management has determined that a principle is not relevant to the associated component. Considerations in applying this judgment may include the entity structure recognizing any legal, regulatory, industry, or contractual requirements for governance of the entity, and the level of use and dependence on technology used by the entity.

100 If management decides that a principle is not relevant, management must support that determination, including the rationale of how, in the absence of that principle, the associated component could be present and functioning. When a relevant principle is deemed not to be present and functioning, a major deficiency exists in the system of internal control.

101 In determining whether a component is present and functioning, senior management and the board of directors need to determine to what extent relevant principles are present and functioning. However, a principle being present and functioning does not imply that the organization strives for the highest level of performance in applying that particular principle. Rather, management exercises judgment in balancing the cost and benefit of designing, implementing, and conducting internal control.

Deficiencies in Internal Control

102 The term “internal control deficiency” refers to a shortcoming in a relevant principle or associated component that has the potential to adversely affect the ability of the entity to achieve its objectives. There are many potential sources for identifying internal control deficiencies, including the entity’s monitoring activities, other components of internal control, and external parties that provide input relative to the presence and functioning of a component or relevant principle. An internal control deficiency or combination of deficiencies that is severe enough to adversely affect the likelihood that the entity can achieve its objectives is referred to as a “major deficiency”.

103 When an organization determines that an internal control deficiency or combination of deficiencies exists, management uses judgment to assess the severity of that deficiency in determining the presence and functioning of the principle, the associated component, and ultimately the entity’s system of internal control. Regulators, standard-setting bodies, and other relevant third parties may establish criteria for evaluating the severity

and corresponding classification and reporting of deficiencies relating to external reporting objectives, operations, and compliance objectives. As well, for internal reporting and other operations objectives, management and board of directors establish objective criteria for evaluating internal control deficiencies and reporting to those responsible for achieving these objectives. The Framework does not prescribe such criteria, but recognizes and accommodates the authority and responsibility of those other parties that interact with the entity to issue such laws, rules, regulations, and standards for conducting assessments and classifications.

104 In those instances where an entity is applying an external law, rule, regulation, or standard, management considers terms relating to internal control deficiencies and the unique considerations of those standards. Management also needs to develop an understanding of any differences between those laws, rules, regulations, and standards when applying the Framework. For instance, regulators prescribe rules for evaluating internal control deficiencies relating to external financial reporting and define terms describing the severity of such deficiencies, which may include material weakness and significant deficiency. For purposes of applying the Framework to external financial reporting, management must apply laws, rules, regulations, and standards appropriate for the entity in evaluating, classifying, and reporting internal control deficiencies.

105 Although the organization may rely on an outsourced service provider to conduct processes, policies, and procedures on behalf of the entity, management retains ultimate responsibility for meeting the requirements set forth in the Framework for an effective system of internal control.

106 Other parties interacting with the entity, such as external auditors and regulators, are not part of the entity's system of internal control and thus cannot be part of management's assessment process.

4. Additional Considerations

Judgment

107 The Framework requires judgment in designing, implementing, and conducting internal control and assessing its effectiveness. The use of judgment enhances management's ability to make better decisions about internal control, but cannot guarantee perfect outcomes.

108 Some of the important areas requiring judgment relate to:

- Applying internal control components relative to categories of objectives
- Applying internal control components and principles within the entity structure
- Specifying suitable objectives and assessing risks
- Assessing whether components are present and operating together
- Assessing whether principles are relevant to the entity and whether relevant principles are present and functioning
- Selecting, developing, and deploying controls necessary to effect principles
- Assessing the severity of one or more deficiencies in internal control both in accordance with the Framework and in connection with applicable laws, rules regulations, and standards.

109 For example, in preparing financial statements, management exercises judgment in complying with external financial reporting requirements. Management considers how identified risks to specified financial reporting objectives and sub-objectives should be managed. Management's alternatives for responding to risks may be more limited compared with some other categories of objectives. That is, management is less likely to accept a risk than to reduce the risk. For external financial reporting objectives relating to published financial statements, risk acceptance or avoidance should occur only when identified risks could not, individually or in aggregate, exceed the risk threshold and result in a material misstatement.

110 Management also exercises judgment in selecting and applying suitable accounting principles, particularly those relating to subjective measurements and complex transactions. For instance, management exercises judgment in making assumptions and using data in developing accounting estimates, in applying accounting principles to complex transactions, and in preparing reliable and transparent presentations and disclosures. Internal control over external financial reporting addresses the potential for bias in exercising judgment that could lead to a material misstatement in external financial reporting.

Points of Focus

111 The Framework describes points of focus that are typically important characteristics of principles. Management is expected to obtain persuasive evidence to support its determination that the components and relevant principles of internal control are present and functioning. To that end, points of focus assist management in designing, implementing, and conducting internal control and in assessing whether the relevant principles are, in fact, present and functioning. The Framework does not require that management assess separately whether points of focus are in place. Instead management considers points of focus in connection with its determination of whether principles are present and functioning.

112 In designing and implementing a system of internal control, management may determine that some of these characteristics are not suitable or relevant and may identify and consider others that are based on specific circumstances of the entity.

113 Management, in its judgment, identifies and considers suitable and relevant points of focus, including those presented in the Framework, that reflect the entity's industry, operating, and regulatory environments. Once management has determined which points of focus are suitable and relevant for a particular principle, those points of focus become important considerations when assessing the presence and functioning of a principle.

114 Points of focus are presented at the beginning of the discussion of the principles within each component chapter.

Controls to Effect Principles

115 Embedded within the internal control process are controls, which consist of policies and procedures. These policies reflect management or board statements of what should be done to effect control. Procedures are actions that implement policies. Organizations select and develop controls within each of the five components to effect relevant principles. Controls are interrelated and may support multiple objectives.

116 The Framework does not prescribe requirements of specific controls that must be selected, developed, and deployed for an effective system of internal control. That determination is a function of management judgment based on factors unique to each entity, such as:

- Laws, rules, regulations, and standards to which the entity is subject
- Nature of the entity's business and the markets in which it operates
- Scope and nature of the management operating model
- Competency of the personnel responsible for internal control
- Use and dependence on technology
- Management's response to assessed risks

117 Management considers controls in conjunction with its assessment of components and relevant principles. Understanding how controls effect principles through their selection, development, and deployment can provide persuasive evidence to support management's assessment of whether the entity's system of internal control is effective. Further, once management has identified controls to effect relevant principles for the entity, the absence of or failure to perform one or more such controls would represent a potential internal control deficiency. The Framework allows judgment in assessing the potential impact of a deficiency on the presence and functioning of a relevant principle. Management may consider alternative controls (whether or not associated with that particular principle) that compensate for the identified deficiency.

Organizational Boundaries

118 Many organizations choose to shift some business activities to outside service providers. This approach has become prevalent because of the benefits of obtaining access to low-cost human resources, reducing costs in the day-to-day management of certain functions, obtaining access to better processes and systems, and allowing management to focus more on the entity's mission.

119 Outsourced service providers can help organizations to perform business processes such as procurement, payables management, payroll, pension and benefit management, investment management, and stock-based compensation programs. Outside service providers may also perform technology activities that support business processes, providing services to procure, manage, and maintain previously internally managed technology systems. Advances in technology have created cost-savings opportunities through access to comprehensive architectures that provide on-demand and scalable shared technology that supports more complex and changing business operations and that may be cost prohibitive for management as an internal investment.

120 This dependence on outsourced service providers changes the risks of business activities, increases the importance of the quality of information and communications from outside the organization, and creates greater challenges in overseeing its activities and related internal controls. While management can use others to execute activities and controls for or on behalf of the entity, it maintains responsibility for the overall system of internal control. For instance, management maintains responsibility for specifying objectives, managing associated risks, establishing mechanisms to support the functioning of the components of internal control, and selecting, developing, and deploying control activities.

121 The Framework can be applied to the entire entity regardless of what choices management makes about how it will execute business activities that support its objectives, either directly or through external relationships.

Technology

122 Technology may be essential to support management's pursuit of the entity's objectives and to better control the organization's activities. The number of entities that use technology continues to grow as does the extent that technology is used in most entities.

123 Technology is often referred to by other terms, such as "management information systems" or "information technology." These terms share the ideas of using a combination of automated and manual processes, and computer hardware and software, methodologies, and processes. The Framework uses the term "technology" to refer to all computerized systems, including software applications running on a computer and operational control systems.

124 Technology environments vary significantly in their size, complexity, and extent of integration. They range from large, centralized, and integrated systems to decentralized systems that operate independently within a specific unit. They may also involve real-time processing environments that enable immediate access to information, including mobile computer applications that can cut across many systems, organizations, and geographies. Technology enables organizations to process high volumes of transactions, transform data into information to support sound decision making, share information efficiently across the entity and with business partners, and secure confidential information from inappropriate use. In addition, technology can allow an entity to share operational and performance data with the public.

125 Technology innovation creates both new opportunities and new risks. It can enable the development of new business markets and models, generate efficiencies through automation, and enable entities to do things that were previously hard to imagine. It may also increase complexity, which makes identifying and managing the risks more difficult.

126 The principles presented in the Framework do not change with the application of technology. This is not to say that technology does not change the internal control landscape. Certainly it affects how an entity implements the components of internal control, such as the greater availability of information and the use of automated procedures, but the principles remain the same.[6]

Larger versus Smaller Entities

127 The seventeen principles underlying the five components of internal control are just as applicable for smaller entities as for larger ones. However, implementation approaches may vary for smaller entities, regardless of whether the entity is publicly traded, privately held, governmental, or not-for-profit. For example, all public companies have boards of directors, or other similar governing bodies, with oversight responsibilities related to reporting. A smaller entity may have a less complex organizational structure and operations, and more frequent communication with directors, enabling a different approach to board oversight. Similarly, while many public companies are often required to have a whistle-blower program, there may be a difference in the reporting procedures between

6 Note that as this is a principles-based framework and because technology is continually evolving, the Framework does not address specific technologies, such as cloud computing or the rise in social media.

other types of small and large entities. In a large entity, for example, the volume of reported events may require initial reporting to an identified internal staff function, but a smaller entity may allow direct reporting to the audit committee chair.

128 Smaller entities typically have unique advantages, which can contribute to effective internal control. These may include a wider span of control by senior management and greater direct interaction with personnel. For instance, smaller companies may find informal staff meetings highly effective for communicating information relevant to operating performance, whereas larger companies may need more formal mechanisms such as written reports, intranet portals, periodic formal meetings, or conference calls to communicate similar matters.

129 Conversely, larger entities may enjoy certain economies of scale, which often affect support functions. For example, establishing an internal audit function within a smaller, domestic entity likely would require a larger percentage of the entity's economic resources than would be the case for a larger, multinational entity. A smaller entity may not have an internal audit function or might rely on co-sourcing or outsourcing to provide needed skills, where the larger entity's function might have a significantly broader range of experienced in-house personnel. But in all likelihood the relative cost for the smaller entity would be higher than for the larger one.

Benefits and Costs of Internal Control

Benefits

130 Internal control provides many benefits to an entity. It provides management and board of directors with added confidence regarding the achievement of objectives, it provides feedback on how a business is functioning, and it helps to reduce surprises. Among the most significant benefits of effective internal control for many entities is the ability to meet certain requirements to access capital markets, providing capital-driven innovation and economic growth. Such access of course comes with responsibilities to effect timely and reliable reporting for shareholders, creditors, capital providers, regulators, and other third parties with which an entity has direct contractual relationships. For instance, effective internal control supports reliable external financial reporting, which in turn enhances investor confidence in providing the requisite capital.

131 Other benefits of effective internal control include:

- Reliable reporting that supports management and board decision making on matters such as product pricing, capital investment, and resource deployment
- Consistent mechanisms for processing transactions, supporting quality of information and communications across an organization, enhancing speed and reliability at which transactions are initiated and settled, and providing reliable recordkeeping and ongoing integrity of data
- Increased efficiency within functions and processes

- A basis for decisions where highly subjective and substantial judgment is needed
- Ability and confidence to accurately communicate business performance with business partners and customers, which supports continuity of the business relationship

132 Entities always have limits on their human and capital resources and constraints on how much they can spend, and therefore they will often consider the costs relative to the benefits of alternative approaches in managing internal control options.

Costs

133 Generally, it is easier to deal with the cost aspect in the cost-benefit equation because in most cases financial costs can be quantified fairly precisely. Usually considered are all direct costs associated with implementing internal control actions and responses, plus indirect costs, where practically measurable. Some entities also include opportunity costs associated with use of resources.

134 Overall, management considers a variety of cost factors in relation to expected benefits when selecting and developing internal controls. These may include:

- Considering the trade-offs between recruiting and retaining staff with a higher level of competency and the related higher compensation costs. For instance, a smaller, stable, privately held company may not want to, or be able to, hire a chief financial officer with the experience of working for a publicly traded company.
- Assessing the efforts required to select, develop, and perform control activities; the potential incremental efforts that the activity adds to the business process; and the efforts to maintain and update the control activity when needed.
- Assessing the impacts of added reliance on technology. While the effort to perform the control and the impact of added technology-based controls on the business process may be small, the cost associated with selecting, developing, maintaining, and updating the technology could be substantial.
- Understanding how changes in information requirements may call for greater data collection, processing, and storage that could trigger exponential growth in data volume. With more data available, an organization faces the challenge of avoiding information overload by ensuring flow of the right information, in the right form, at the right level of detail, to the right people, at the right time. Establishing an information system that balances costs and benefits depends on thoughtful consideration of information requirements.

Other Considerations in Determining Benefits and Costs

135 The benefit side of the cost-benefit equation often involves even more subjective evaluation. For example, benefits of effective training programs usually are apparent but difficult to quantify. Training programs are not often designed to measure the benefits or to capture the necessary data to evaluate the program. Sales training programs may not be structured to measure before-and-after employee sales results, making it difficult to determine whether the training is effective and accomplishing its objectives. Further, evaluating the benefits in relation to stakeholder expectations may be more difficult to assess. In many cases, however, the benefit of developing actions within any of the five components of internal control can be evaluated in the context of the benefit associated with achievement of the related objective.

136 The complexity of cost-benefit determinations is compounded by the interrelationship of controls with business operations. Where controls are integrated with management and business processes, it is difficult to isolate either their costs or benefits.

137 It is up to management to decide how an entity evaluates the costs versus benefits of alternative approaches to implementing a system of internal control, and what action it ultimately takes. However, cost alone is not an acceptable reason to avoid implementing internal controls. The cost versus benefits considerations support management's ability to develop and maintain a system of internal control that balances the allocation of human resources in relation to the areas of greatest risk, complexity, or other factors relevant to the entity's objectives.

Documentation

138 Entities develop and maintain documentation for their internal control system for a number of reasons. One is to provide clarity around roles and responsibilities, which promotes consistency in adhering to desired practices in managing the business. Effective documentation assists in capturing the design of internal control and communicating the who, what, when, where, and why of internal control execution, and creates standards and expectations of performance and conduct. Another purpose of documentation is to assist in training new personnel and to offer a refresher or reference for other employees. Documentation also provides evidence of the performance of activities that are part of the system of internal control, enables proper monitoring, and supports reporting on internal control effectiveness, particularly when evaluated by other parties interacting with the entity, such as regulators, auditors, or customers. Documentation also provides a means to retain organizational knowledge and mitigate the risk of having the knowledge within the minds of a limited number of employees.

139 Management must also determine how much documentation is needed to assess the effectiveness of internal control. Some level of documentation is always necessary to assure management that the components of internal control are in place and functioning. This may include, for example, documents showing that all shipments are billed or that periodic reconciliations are performed. Two specific levels of documentation requirements must be considered in relation to external financial and non-financial reporting:

- In cases where management asserts to regulators, shareholders, or other third parties on the design and operating effectiveness of its overall system of internal control, management has a higher degree of responsibility. Typically, this requires documentation to support the assertion that all components of internal control are in place and functioning. The nature and extent of the documentation may be influenced by the entity's regulatory requirements. This does not necessarily mean that all documentation is or should be more formal, but that persuasive evidence to show that the components of internal control are present and operating together is available and appropriate to satisfy the entity's objectives.
- In cases where an external auditor attests to the effectiveness of the overall system of internal control, management will likely be expected to provide the auditor with support for its assertion on the effectiveness of internal control. That support includes evidence that the system of internal control is properly designed and operating effectively to provide reasonable assurance of achieving the entity's objective. In considering the nature and extent of documentation needed, management should remember that the documentation to support the assertion will likely be used by the external auditor as part of his or her audit evidence. Management would also need to document significant judgments, how such decisions were considered, and how the final decisions were reached.

140 There may still be instances where internal control is informal and undocumented. This may be appropriate where management is able to obtain evidence captured through the normal conduct of the business that indicates personnel regularly performed those controls. However, it is important to keep in mind that control processes, such as monitoring activities or risk assessments, cannot be performed entirely in the minds of the senior management without some documentation of management's thought process and analyses.

141 The level and nature of documentation can also vary by the size of the organization and the complexity of the control. Larger entities usually have a more extensive system of internal control and greater complexity in business processes, and therefore typically find it necessary to have more extensive documentation, such as in-depth policy and procedure manuals, flowcharts of processes, organizational charts, and job descriptions. Smaller entities often find less need for formal documentation. In smaller companies, typically there are fewer people and levels of management, closer working relationships, and more frequent interaction, all of which promote communication of what is expected and what is being done. Consequently, management of a smaller entity can often determine that controls are functioning through direct observation.

142 Documentation of internal control should meet business needs and be commensurate with circumstances. The extent of documentation supporting the design and operating effectiveness of the five components of internal control is a matter of judgment, and should be done with cost-effectiveness in mind. In addition, the organization may benefit from some form of formal documentation that enables management to reflect on the rationale for the judgment and alignment with entity objectives.

5. Control Environment

Chapter Summary

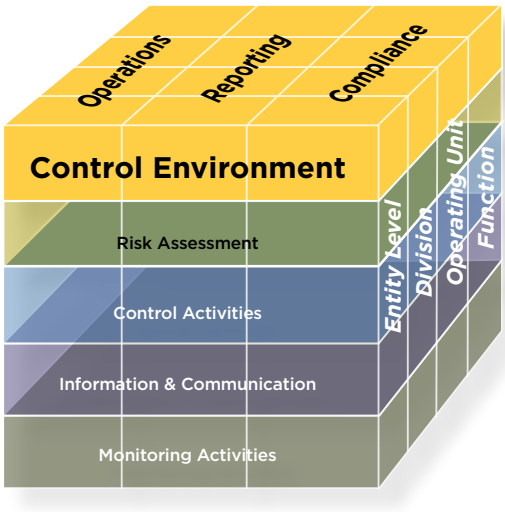
143 The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The board of directors and senior management establish the tone at the top regarding the importance of internal control including expected standards of conduct. Management reinforces expectations at the various levels of the organization. The control environment comprises the integrity and ethical values of the organization; the parameters enabling the board of directors to carry out its oversight responsibilities; the organizational structure and assignment of authority and responsibility; the process for attracting, developing, and retaining competent individuals; and the rigor around performance measures, incentives, and rewards to drive accountability for performance. The resulting control environment has a pervasive impact on the overall system of internal control.

Principles relating to the Control Environment component

1. The organization demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Introduction

144 The control environment is influenced by a variety of internal and external factors, including the entity's history, values, market, and the competitive and regulatory landscape. It is defined by the standards, processes, and structures that guide people at all levels in carrying out their responsibilities for internal control and making decisions. It creates the discipline that supports the assessment of risks to the achievement of the entity's objectives, performance of control activities, use of information and communication systems, and conduct of monitoring activities.



145 An organization that establishes and maintains a strong control environment positions itself to be more resilient in the face of internal and external pressures. It does this by demonstrating behavior consistent with the organization's commitment to integrity and ethical values, adequate oversight processes and structures, organizational design that enables the achievement of the entity's objectives with appropriate assignment of authority and responsibility, a high degree of competence, and a strong sense of accountability for the achievement of objectives.

146 Organizational culture supports the control environment insofar as it sets expectations of behavior that reflects a commitment to integrity and ethical values, oversight, accountability, and performance evaluation. Establishing a strong culture considers, for example, how clearly and consistently ethical and behavioral standards are communicated and reinforced in practice. As such, culture is part of an organization's control environment, but also encompasses elements of other components of internal control, such as policies and procedures, ease of access to information, and responsiveness to results of monitoring activities. Therefore culture is influenced by the control environment and other components of internal control, and vice versa.

Demonstrates Commitment to Integrity and Ethical Values

Principle 1: The organization demonstrates a commitment to integrity and ethical values.

Points of Focus

147 The following points of focus may assist management in determining whether this principle is present and functioning:

- **Sets the Tone at the Top**—The board of directors and management at all levels of the entity demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.
- **Establishes Standards of Conduct**—The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the organization and by outsourced service providers and business partners.
- **Evaluates Adherence to Standards of Conduct**—Processes are in place to evaluate the performance of individuals and teams against the entity's expected standards of conduct.
- **Addresses Deviations in a Timely Manner**—Deviations of the entity's expected standards of conduct are identified and remedied in a timely and consistent manner.

Tone at the Top and throughout the Organization

148 Management and the board of directors or equivalent oversight body are expected to lead by example in developing values, a philosophy, and an operating style for the organization. They take into account the expectations of the entity's various stakeholders, such as employees, suppliers, customers, investors, and the wider community. Further, they are influenced by the social and ethical norms in the markets where the entity operates. In addition to fostering an understanding and adherence to legal and regulatory requirements, management and the board take specific measures to set the tone in terms of moral, social, environmental, or other forms of responsible conduct, such as greenhouse gas emissions reporting, sustainable production processes, or community outreach after natural disasters. The resulting expectations are expressed to varying degrees of formality in the form of:

- Mission and values statements
- Standards or codes of conduct
- Policies and practices
- Operating principles
- Directives, guidelines, and other supporting communications
- Actions and decisions of management at various levels and the board of directors
- Attitudes and responses to deviations from expected standards of conduct
- Informal and routine actions and communication of leaders at all levels of the entity

149 These elements reflect the expectations of integrity and ethical values and the degree to which they are applied in decisions made at all levels of the organization, by outsourced service providers, and by business partners (e.g., joint venture partners, strategic alliances). They articulate and reinforce the commitment to doing what is right, not just what complies with laws and regulations, so that these priorities are understood and embraced by all stakeholders. The degree to which these expectations are not only communicated but also applied by senior management and the board as well as all other levels of leadership within the organization characterizes the tone at the top and throughout the organization.

150 Tone is impacted by the operating style and personal conduct of management and the board of directors, attitudes toward risk, and positions, which may be conservative or aggressive (e.g., position on estimates, policy choices), degree of formality (e.g., in a smaller family business, controls may be more informal), all of which sends a message to the organization. Personal indiscretions, lack of receptiveness to bad news, or unfairly balanced compensation practices could impact the culture and ultimately provide an incentive for inappropriate conduct. In contrast, a history of ethical and responsible behavior by management and the board of directors and demonstrated commitment to addressing misconduct send strong messages in support of integrity. Employees are likely to develop the same attitudes about right and wrong—and about risks and controls—as those shown by management. Individual behavior is often influenced by the knowledge that the chief executive officer has behaved ethically when faced with a tough business-based or personal decision, and that all managers have taken timely action to address misconduct.

151 The tone must be consistent from senior management through to operating unit management levels to ensure that the values, business drivers, and resulting behavior are shared by all employees and partners of the organization. This includes the various layers and divisions sometimes referred to as “tone in the middle” in larger organizations. Such consistency helps pull the organization together in the pursuit of the entity’s objectives. However, challenges to such consistency can arise in various forms. For instance, operating in different markets may call for different motivational approaches, different degrees of evaluation of suppliers, and different customer service levels—creating different tones at different levels of the organization. The messages

from management about what is or is not acceptable may vary to impact the intended audience, but the more they remain consistent with the tone at the top, the more homogenous the performance of internal control responsibilities in the pursuit of the entity's objectives will be.

152 In some cases, the tone set by the chief executive may result in unintended consequences. Consider, for example, a management team that readily modifies the entity's standard contractual terms to compete in the local business environment. While such modification may be seen as positive for purposes of satisfying customer needs and generating revenue—for instance getting products to customers faster—it may be detrimental to the achievement of other objectives, such as complying with product safety standards, quotas, fair sales practices, or other requirements. Clear guidance and direction from the top, as well as congruence across different levels of management, are fundamental to the achievement of the entity's objectives.

153 Tone at the top and throughout the organization is fundamental to the functioning of an internal control system. Without a strong tone at the top to support a strong culture of internal control, awareness of risk can be undermined, responses to risks may be inappropriate, control activities may be ill-defined or not followed, information and communication may falter, and feedback from monitoring activities may not be heard or acted upon. Therefore tone can be either a driver or a barrier to internal control.

Standards of Conduct

154 Standards of conduct guide the organization in behaviors, activities, and decisions in the pursuit of its objectives by:

- Establishing what is right and wrong
- Providing guidance for navigating what lies in between, considering associated risks
- Reflecting governing laws, rules, regulations, standards, and other expectations that the organization's stakeholders may have, such as corporate social responsibility

155 Ethical expectations, norms, and customs can vary across borders. Management and the board of directors or equivalent oversight body establish the standards and mechanisms for the organization to understand and adhere to doing what is right, and define the process and resources for interpreting and addressing the potential for deviations. These expectations are translated into an organizational statement of beliefs, values, and standards of conduct.

156 The organization demonstrates its commitment to integrity and ethical values by applying the standards of conduct and continually asking challenging questions, particularly when faced with difficult decisions. For example, it might ask: Does it infringe on the organization's standards of conduct? Is it legal? Would we want our shareholders, customers, regulators, suppliers, or other stakeholders to know about it? Would it reflect negatively on the individual or the organization?

157 Integrity and ethical values are core messages in the organization's communications and training. For example, a company that regularly receives awards for "best places to work" and achieves high employee retention rates typically provides training on corporate ethical values and organizational culture, with the support of senior management and the board. The training sessions are conducted quarterly or biannually depending on the number of new employees hired. During such training, employees learn how the ethical climate has developed in the organization. In addition, employees are provided with examples of how integrity and ethical values have assisted in identifying issues and solving problems and the importance of speaking up and raising concerns.

158 The organization's standards of conduct are continually communicated and reinforced not only to all levels of the organization but also to outsourced service providers. For example, enforcing internal control for compliance with product safety standards extends beyond the entity to include joint venture partners, suppliers, sales distributors, and other outsourced service providers at all locations.

159 Management retains ultimate accountability for activities it delegates through legal or contractual arrangements to outsourced service providers. Variables that can affect the extent of communications, oversight, and other activities needed to ensure that outsourced service providers and business partners adhere to the entity's standards of conduct include:

- The nature of services outsourced
- Extent of alignment of the service provider's standards of conduct with those of the entity
- Quality and frequency of the service provider's reinforcement and oversight of adherence to standards of conduct by its personnel
- Magnitude and level of complexity of the entity's supply chain and business model

160 Inappropriate conduct by outsourced service providers or business partners can reflect negatively on senior management and impact the entity itself by causing harm to customers, other stakeholders, or the reputation of the organization, requiring costly corrective action. Therefore management retains responsibility for the performance of processes that it has delegated to outside service providers or business partners.

Adherence and Deviations

161 The established standards of conduct provide the basis for evaluating adherence to integrity and ethical values across the organization and its outsourced service providers. They are communicated through the organization's policies and practices, and employment or service contracts. Some organizations require formal acknowledgment of receipt and compliance with such standards. To gain assurance that the standards are being followed in practice, the actions, decisions, and attitudes of individuals are evaluated by management or an independent party.

162 The lack of adherence to standards of conduct often stems from situations such as:

- Tone at the top that does not effectively convey expectations regarding adherence to standards
- A board of directors that does not provide impartial oversight of senior management's adherence to standards
- High decentralization without adequate oversight, leaving senior management unaware of actions taken at lower levels
- Coercion by superiors, peers, or external parties to cut corners or engage in fraud or other illicit behavior
- Performance goals that create incentives or pressures to compromise ethical behavior
- Inadequate vehicles by which employees can safely voice questions and concerns
- Failure to address non-existent or ineffective controls, which allow opportunities to conceal poor performance
- Inadequate process for the investigation and resolution of alleged misconduct
- A weak internal audit function that does not have the ability to detect and report improper conduct
- Penalties for improper conduct that are inconsistently applied, insignificant, or unpublicized and thus lose their deterrent value

163 For example, standards of conduct may prohibit practices that could be perceived as collusion to fix prices, but the organization must establish mechanisms to enforce standards, such as awareness communications and training, scanning market pricing activity to identify potential issues, and other measures to prevent or detect a deviation from the organization's standards of conduct. The organization communicates established tolerance levels for deviations. Depending on the significance of the impact to the organization, the level of remedial action may vary but is applied consistently across the organization. Evaluations of individual and team adherence to standards of conduct are part of a systematic process for escalation and resolution of exceptions. The process requires that management:

- Define a set of indicators (e.g., training completion rates, results of monitoring activities, breaches of confidentiality, collusion with other market participants, harassment cases) to identify issues and trends related to the standards of conduct for the organization, including its outsourced service providers. Such indicators are revisited periodically and refined as necessary to help raise potential issues early or before they repeat themselves.
- Establish continual and periodic compliance procedures to confirm that expectations and requirements are being met both internally and by outsourced service providers.

- Identify, analyze, and report business conduct issues and trends to senior management and the board of directors. Mechanisms for identifying issues include direct reporting lines, human resource functions, and hotlines. Analysis often requires cross-functional teams to determine the root cause and what corrective actions are needed.
- Consider the strength of leadership in the demonstration of integrity and ethical values as an evaluated behavior in performance reviews, compensation, and promotion decisions.
- Compile allegations centrally and have these evaluated by individuals independent of the allegation.
- Conduct and document investigations based on defined investigation protocols.
- Follow through on the implementation of corrective actions so that issues are remedied in a timely and consistent manner.
- Periodically analyze of issues to identify trends and root causes, calling for modification of policy, communications, training, or controls.

164 Evaluations may be conducted by an ongoing management process and/or by an independent party. Individuals can also assess and report irregularities through formal and informal communication channels, such as a whistle-blowing program, an ethics hotline, upward feedback processes, and regular staff meetings.

165 Deviations from expected standards of conduct are addressed in a timely and consistent manner. Depending on the severity of the deviation determined through the evaluation process, management may take different actions and may also need to consider local laws, but the standards to which it holds employees remain consistent. Depending on the severity of the deviation, the employee may be issued a warning and provided coaching, put on probation, or terminated.

Exercises Oversight Responsibility

Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Points of Focus

166 The following points of focus may assist management in determining whether this principle is present and functioning:

- **Establishes Oversight Responsibilities**—The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations.
- **Applies Relevant Expertise**—The board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate actions.
- **Operates Independently**—The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.
- **Provides Oversight for the System of Internal Control**—The board of directors retains oversight responsibility for management's design, implementation, and conduct of internal control:
  - *Control Environment*—Establishing integrity and ethical values, oversight structures, authority and responsibility, expectations of competence, and accountability to the board.
  - *Risk Assessment*—Overseeing management's assessment of risks to the achievement of objectives, including the potential impact of significant changes, fraud, and management override of internal control.
  - *Control Activities*—Providing oversight to senior management in the development and performance of control activities.
  - *Information and Communication*—Analyzing and discussing information relating to the entity's achievement of objectives.
  - *Monitoring Activities*—Assessing and overseeing the nature and scope of monitoring activities and management's evaluation and remediation of deficiencies.

Authorities and Responsibilities

167 The board of directors or equivalent oversight body understands the business and expectations of stakeholders, including customers, employees, investors, and the general public, as well as legal and regulatory requirements and related risks. These expectations and requirements help shape the objectives of the organization, oversight responsibilities of the board, and resource requirements.

168 The board has the authority to hire as well as terminate, as necessary, and establish succession planning for the chief executive officer or equivalent, who is then charged with overall execution of the entity's strategy, achievement of its objectives, and effectiveness of the system of internal control. The board is responsible for providing oversight and constructive challenge to management.

169 Depending on the jurisdiction, oversight structures are developed voluntarily or as mandated by law, regulation, or standards, such as stock exchange listing standards. While requirements for privately owned, not-for-profit, or other entities may vary, publicly listed companies in many jurisdictions require committees at the board level to focus on specialized topics, such as:

- Nomination/governance committees to lead the selection of directors and oversee the evaluation of senior management and the board of directors
- Compensation committees to oversee policies and practices for senior management compensation, motivating expected behaviors, balancing incentives for short- and long-term performance, linking performance to strategic objectives, and relating compensation to risk
- Audit committees to oversee internal control over financial reporting and the integrity and transparency of external reporting, including financial reports
- Other committees of the board dedicated to address specific matters that are critical to the entity's objectives (e.g., risk committees for financial services institutions or compliance committees for pharmaceutical companies)

170 Board oversight is supported by structures and processes that management establishes at a business-execution level. For instance, management committees may focus on topics such as information technology, products/services, process, or other aspects of the business requiring dedicated focus. Management continually assesses risks posed by the changes in the operating environment (e.g., emergence of new technology, heightened regulatory requirements, and business model evolution) and addresses the implications for the internal control system.

171 While the board of directors retains oversight responsibility, the chief executive officer and senior management bear direct responsibility for developing and implementing the internal control system. Depending on the type of organization and its strategy, structure, and objectives, operating units may have more or less autonomy designing the processes and structures to enable internal control. For example, while one organization may implement an enterprise resource planning system that standardizes all major processes and controls, another organization may leave it to each division to determine and implement those most suitable to its business activities.

Independence and Relevant Expertise

172 The board of directors is independent from management and demonstrates relevant skills and expertise in carrying out its oversight responsibilities. Independence is demonstrated in the board member's objectivity of mind, action, appearance, and fact. Publicly listed companies are typically required to have a majority of its directors be independent and with no current or recent personal or professional relationship with the entity. (In some jurisdictions, this is also a requirement for all members of some committees of the board, such as audit committees.) The factor of independence and relevant expertise also considers the various board seats held by each of the board members to limit any bias or conflict of interest that could result from board members sitting on other company boards.

173 Because a board must be actively engaged at all times and be prepared to question and scrutinize management's activities, present alternative views, and have the courage to act in the face of obvious or suspected wrongdoing, it is necessary that the board include independent directors. Certainly, officers and employees bring deep knowledge of the entity to the table, but independent directors with relevant expertise provide value through their impartiality, healthy skepticism, and unbiased evaluation.

174 Privately owned, not-for-profit, or other entities may find it costly or otherwise difficult to attract competent independent directors. Depending on applicable requirements (some may not be required to have a board of directors), it may be incumbent on these organizations to identify professional and personal qualities of the candidate important to the entity (e.g., understanding of stakeholder perspectives, internal control mindset) and establish a board with members who demonstrate these qualities. Those entities that are unable to have an independent board recognize this factor and rely on different processes and controls that result in adequate oversight of the entity.

175 Board composition is determined considering the mission, values, and various objectives of the entity as well as the skills and expertise needed to oversee, probe, and evaluate the senior management team most appropriately. The size of the board is determined by considering the appropriate number of members to adequately facilitate constructive criticisms, discussions, and decision making. Capabilities expected of all board members include integrity and ethical standards, leadership, critical thinking, and problem-solving. Further, the board is expected to include more specialized skills and expertise, with sufficient overlap to enable discussion and deliberation, such as:

- Internal control mindset (e.g., professional skepticism, perspectives on approaches for identifying and responding to risks, and assessing the effectiveness of the system of internal control)
- Market and entity knowledge (e.g., knowledge of products/services, value chain, customer base, competitors)
- Financial expertise, including financial reporting (e.g., accounting standards, financial reporting requirements)
- Legal and regulatory expertise (e.g., understanding of governing laws, rules, and standards)

- Social and environmental expertise (e.g., understanding of expectations of social and environmental expectations and activities)
- Incentives and compensation (e.g., knowledge of market compensation rates and practices)
- Relevant systems and technology (e.g., understanding critical systems and technology challenges and opportunities)

176 The expertise and independence of the board of directors are evaluated regularly in relation to the evolving needs of the entity. Board members participate in training as appropriate to keep their skills and expertise current and relevant. Below is an example of the board of directors activities involved in exercising oversight for the development and performance of internal control through each of the five components of the Framework.

Internal Control Component	Oversight Activities of the Board
Control Environment	• Oversee the definition of and apply the standards of conduct of the organization • Establish the expectations and evaluate the performance of the chief executive officer or equivalent role • Establish oversight structures and processes aligned with the objectives of the entity (e.g., board and committees as appropriate with requisite skills and expertise) • Commission board oversight effectiveness reviews and addresses opportunities for improvement • Exercise fiduciary responsibilities to shareholders or other owners (as applicable) and due care in oversight (e.g., prepare for and attend meetings, review the entity's financial statements and other disclosures) • Challenge senior management by asking probing questions about the entity's plans and performance, and requiring follow-up and corrective actions, as necessary (e.g., questioning transactions that occur repeatedly at the end of interim or annual reporting periods)
Risk Assessment	• Consider internal and external factors that pose significant risks to the achievement of objectives; identify issues and trends (e.g., sustainability implications of the entity's business operations) • Discuss management's assessment of risks to the achievement of objectives, including the potential impact of significant changes (e.g., risks associated with entering a new market), and fraud or corruption • Evaluate how proactively the organization manages innovations and changes such as those triggered by new technology or economic and geopolitical shifts

Internal Control Component	Oversight Activities of the Board
Control Activities	• Make specific inquiries of management regarding the selection, development, and deployment of control activities in significant risk areas and remediation as necessary (e.g., in response to significant risks emerging from internal or external factors) • Oversee senior management in its performance of control activities
Information and Communication	• Communicate direction and tone at the top • Obtain, review, and discuss information relating to the entity's achievement of objectives • Scrutinize information provided and present alternative views • Review disclosures to external stakeholders for completeness, relevance, and accuracy • Allow for and address upward communication of issues
Monitoring Activities	• Assess and oversee the nature and scope of monitoring activities, any management overrides of controls, and management's evaluation and remediation of deficiencies • Evaluate the integrity and ethical values of senior management • Engage with management, internal and external auditors, and others, as appropriate, to evaluate the level of awareness of the entity's strategies, specified objectives, risks, and control implications associated with evolving business, infrastructure, regulations, and other factors

177 Transparency obligations reinforce accountability of both senior management and the board of directors. While disclosure requirements and expectations may differ by jurisdiction, industry, or otherwise, the board of directors oversees that such needs are understood and met over time. Reporting to the board of directors occurs both on a regular and ad hoc basis, as needed, to help the board oversee the issues relating to the system of internal control.

Establishes Structure, Authority, and Responsibility

Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

Points of Focus

178 The following points of focus may assist management in determining whether this principle is present and functioning:

- **Considers All Structures of the Entity**—Management and the board of directors consider the multiple structures used (including operating units, legal entities, geographic distribution, and outsourced service providers) to support the achievement of objectives.
- **Establishes Reporting Lines**—Management designs and evaluates lines of reporting for each entity structure to enable execution of authorities and responsibilities and flow of information to manage the activities of the entity.
- **Defines, Assigns, and Limits Authorities and Responsibilities**—Management and the board of directors delegate authority, define responsibilities, and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the organization:
  - *Board of Directors*—Retains authority over significant decisions and reviews management's assignments and limitations of authorities and responsibilities.
  - *Senior Management*—Establishes directives, guidance, and control to enable management and other personnel to understand and carry out their internal control responsibilities.
  - *Management*—Guides and facilitates the execution of senior management directives at entity and its subunits.
  - *Personnel*—Understands the entity's standard of conduct, assessed risks to objectives, and the related control activities at their respective levels of the entity, the expected information and communication flow, and monitoring activities relevant to their achievement of the objectives.
  - *Outsourced Service Providers*—Adheres to management's definition of the scope of authority and responsibility for all non-employees engaged.

Organizational Structures and Reporting Lines

179 Senior management and the board of directors establish the organizational structure and reporting lines necessary to plan, execute, control, and periodically assess the activities of the entity, in other words carry out their oversight responsibilities. They are supported by requisite processes and technology to provide for clear accountability and information flows within and across the overall entity and its subunits.

180 Entities are often structured along various dimensions. In particular:

- The management operating model may follow product or service lines to facilitate development of new products and services, optimize marketing activities, rationalize production, and improve customer service or other operational aspects.
- Legal entity structures are often designed to manage business risks, create favorable tax structures, and empower managers at foreign operations.
- Geographic markets may provide for further subdivisions or aggregations of performance.
- Entities also enter into a variety of relationships with outsourced service providers to support the achievement of objectives, which creates additional structures and reporting lines.

181 Each of these lenses can yield a different evaluation of the system of internal control. While the aggregation of risks along one dimension may indicate no issues, the view along a different dimension may show concentration risk around certain customer types, overreliance on a sole vendor, or other vulnerabilities. Ownership and accountability at each level of aggregation enables such multidimensional review and analysis.

182 Organizational structures evolve as the nature of the business evolves. Management therefore reviews and evaluates the structures for continued relevance and effectiveness and efficiency in support of the internal control system. Consider, for example, a bank that reports performance results and internal control effectiveness by legal entity, business unit, or geography. If it does not regularly revisit its reporting to verify that it adequately reflects its current business model, it may fail to recognize the emergence of certain risks, the absence of appropriate controls, and inadequacy of reporting.

183 For each type of structure it operates, management designs and evaluates the lines of reporting so that responsibilities are carried out and information flows as needed (e.g., geographic market structure, business segment structure, legal entity structure). It also verifies there is no conflict of interest inherent in the execution of responsibilities across the organization and its outsourced service providers. Variables to consider when establishing and evaluating organizational structures include the following:

- Nature, size, and geographic distribution of the entity's business
- Risks related to the entity's objectives and business processes, which may be retained internally or outsourced, and interconnections with outsourced service providers and business partners

- Nature of the assignment of authority and responsibility to top, operating unit, functional, and geographic management
- Definition of reporting lines (e.g., direct reporting/"solid line" versus secondary report/"dotted line") and communication channels
- Financial, tax, regulatory, and other reporting requirements of relevant jurisdictions

184 Regardless of the organizational structure, definitions, and assignments of authority and responsibility, reporting lines and communication channels must be clear to enable accountability over operating units and functional areas. For example, the board determines which senior management roles have at least a "dotted line" to the board of directors to allow for open communication to the board of all issues of importance. Similarly, direct reporting and informational reporting lines are defined at all levels of the organization.

185 Responsibilities can generally be viewed as falling within three lines of defense against the failure to achieve the entity's objectives, with oversight by the board of directors:

- Management and other personnel on the front line provide the first line of defense in day-to-day activities. They are responsible for maintaining effective internal control day to day; they are compensated based on performance in relation to all applicable objectives.
- Business-enabling functions (also referred to as support functions) provide guidance on internal control requirements and evaluating adherence to defined standards; while they are functionally aligned to the business, their compensation is not directly tied to performance of the area to which they render expert.
- Internal auditors provide the third line of defense in assessing and reporting on internal control and recommending corrective actions or enhancements for management consideration and implementation; their position and compensation are separate and distinct from the business areas they review.

186 Periodic evaluation of existing structures in relation to the achievement of the entity's objectives enables realignment with emerging priorities (e.g., new regulations) and rationalization (e.g., cutting across silos of different functions or operating units) to provide for a comprehensive and integrated view of internal control.

Authorities and Responsibilities

187 The board of directors delegates authority and defines and assigns responsibility for senior management. In turn, senior management delegates authority and defines and assigns responsibility at the overall entity and its subunits. Authority and responsibility are delegated based on demonstrated competence, and roles are defined based on who is responsible for or kept informed of decisions. The board and/or senior management define the degree to which individuals and teams are authorized and encouraged, or limited, to pursue achievement of objectives or address issues as they arise.

188 Key roles and responsibilities assigned across the organization typically include the following:

- The board of directors stays informed and challenges senior management as necessary to provide guidance on significant decisions.
- Senior management, which includes the chief executive officer or equivalent organizational leader and senior management team, is ultimately responsible to the board of directors and other stakeholders for establishing directives, guidance, and control to enable management and other personnel to understand and carry out their responsibilities.
- Management, which includes supervisors and decision-makers, executes senior management directives at the entity and its subunits.
- Personnel, which includes all employees of the entity, are expected to understand the entity's standards of conduct, objectives as defined in relation to their area of responsibility, assessed risks to those objectives, related control activities at their respective levels of the entity, information, and communication flow, and any monitoring activities relevant to achieving objectives.
- The organization provides personnel with direct responsibility over outsourced processes conducted by service providers. Outsourced service providers are provided with clear and concise contractual terms related to the entity's objectives and expectations of conduct and performance, competence levels, expected information, and communication flow. They may execute business processes on behalf of or together with management, who remains responsible for internal control.

189 Organizations delegate authority and responsibility to enable management and other personnel to make decisions according to management's directives toward the achievement of the entity's objectives. An organization may define or revisit its structures by reducing layers of management, delegating more authority and responsibility to lower levels, or partnering with other organizations. For example, a sales organization may empower its managers to sell at a greater discount to gain market share. However, the authority and responsibility would be delegated only to those who demonstrate the competence to make adequate decisions, consistently adhere to the entity's standards of conduct, policies and procedures, and understand the consequences of the risks they take.

190 Delegation of authority provides for greater agility, but it also increases the complexity of risks to be managed. Senior management, with guidance from the board of directors, provides the basis for determining what is or is not acceptable, such as non-compliance with the organization's regulatory or contractual obligations.

Limitation of Authority

191 Delegating authority empowers people to act as needed in a given role, but it is also necessary to outline the limitations of authority. Authority is limited as necessary so that:

- Delegation occurs only to the extent required to achieve the entity's objectives (e.g., review and approval of new products involves the requisite business and support functions, separate from the sales execution team).
- Decision making is based on sound practices for identifying and assessing risks (e.g., sizing risks and weighing potential losses versus gains in determining which risks to accept and how they are to be managed).
- Duties are segregated to reduce the risk of inappropriate conduct in the pursuit of objectives, and requisite checks and balances occur from the highest to the lowest levels of the organization (e.g., defining roles, responsibilities, and performance measures in a manner to reduce any potential for conflicts of interest).
- Technology is leveraged as appropriate to facilitate the definition and limitation of roles and responsibilities within the workflow of business processes (e.g., different access levels to enterprise resource planning systems at corporate and subsidiary levels, access privileges granted to on-line customers, business partners, and others).
- Third-party service providers who are tasked with carrying out activities on behalf of an entity understand the extent of their decision-making capabilities.

Demonstrates Commitment to Competence

Principle 4: The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

Points of Focus

192 The following points of focus may assist management in determining whether this principle is present and functioning:

- **Establishes Policies and Practices**—Policies and practices reflect expectations of competence necessary to support the achievement of objectives.
- **Evaluates Competence and Addresses Shortcomings**—The board of directors and management evaluate competence across the organization and in outsourced service providers in relation to established policies and practices, and acts, as necessary to address shortcomings.
- **Attracts, Develops, and Retains Individuals**—The organization provides the mentoring and training needed to attract, develop, and retain sufficient and competent personnel and outsourced service providers to support the achievement of objectives.
- **Plans and Prepares for Succession**—Senior management and the board of directors develop contingency plans for assignments of responsibility important for internal control.

Policies and Practices

193 Policies and practices are the entity-level guidance and behavior that reflect the expectations and requirements of investors, regulators, and other stakeholders. They provide the foundation for defining the competence needed within the organization and provide the basis for more detailed procedures for executing and evaluating performance as well as determining remedial actions, as necessary. Such policies and practices provide:

- Requirements and rationale (e.g., implications of product safety laws, rules, regulations, and standards for the entity)
- Skills and conduct necessary to support internal control in the achievement of the entity's objectives (e.g., knowledge of the operation of technology platforms underpinning business processes)
- Defined accountability for performance of key business functions (e.g., defined owners of product safety and areas of applicability within the organization)

- Basis for evaluating shortcomings and defining remedial actions, as necessary (e.g., correcting a process or strengthening the skills of management and other personnel)
- Means to react dynamically to change (e.g., linkage to applicable operating procedures to reflect new regulatory requirements, new risks identified, or internal decision to modify business processes)

194 Policies and practices enable the focus on competence to permeate the organization, starting with the board of directors relative to the chief executive officer, the chief executive officer relative to senior management, and cascading down to various levels of management. The resulting commitment to competence facilitates measuring the achievement of objectives at all levels of the organization and by outsourced service providers by establishing how processes should be carried out and what skills and behavior should be applied.

Commitment to Competence

195 Competence is the qualification to carry out assigned responsibilities. It requires relevant skills and expertise, which are gained largely from professional experience, training, and certifications. It is expressed in the attitude and behavior of individuals as they carry out their responsibilities.

196 The human resources function of an organization can often help define competence and staffing levels by job role, facilitating training and maintaining completion records, and evaluating the relevance and adequacy of individual professional development in relation to the entity's needs.

197 The organization defines competence requirements as needed to support the achievement of objectives, considering, for instance:

- Knowledge, skills, and experience needed
- Nature and degree of judgment and limitations of authority to be applied to a specific position
- Cost-benefit analysis of different levels of skills and experience

198 The board of directors evaluates the competence of the chief executive officer and, in turn, management evaluates competence across the organization and outsourced service providers in relation to established policies and practices, and then acts as necessary to address any shortcomings or excesses. In particular, a changing risk profile may cause the organization to shift resources toward areas of the business that require greater attention. For example, as a company brings a new product to market, it may elect to increase staffing in its sales and marketing teams, or as a new applicable regulation is issued, it may focus on those individuals responsible for implementation. Shortcomings may arise relating to staffing levels, expertise, or a combination of factors. Management is responsible for acting on such shortcomings in a timely manner.

Attracting, Developing, and Retaining Individuals

199 The commitment to competence is supported by and embedded in the human resource management processes for attracting developing, evaluating, and retaining the right fit of management, other personnel, and outsourced service providers. The adequate number of resources is determined and periodically readjusted considering the relative importance of risks to be mitigated to support the achievement of the entity's objectives. Management at different levels establishes the structures, and processes to:

- *Attract*—Conduct formal, in-depth employment interviews to describe the entity's history, culture, and operating style, run background/reference checks, and conduct procedures to determine whether a particular candidate fits with the organizational needs and has the competence for the proposed role.
- *Train*—Enable individuals to develop competencies appropriate for assigned roles and responsibilities, reinforce standards of conduct and expected levels of competence for particular assignments, tailor training based on roles and needs, and consider a mix of delivery techniques, including classroom instruction, self-study, and on-the-job training.
- *Mentor*—Provide guidance on the individual's performance toward expected standards of conduct and competence, align the individual's skills and expertise with the entity's objectives, and help personnel adapt to an evolving environment.
- *Evaluate*—Measure the performance of individuals in relation to the achievement of objectives and demonstration of expected conduct, and against service-level agreements or other agreed-upon standards for recruiting and compensating outsourced service providers.
- *Retain*—Provide incentives to motivate and reinforce expected levels of performance and desired conduct, including training and credentialing as appropriate.

200 Through this process, any behavior not consistent with standards of conduct, policies and practices, and internal control responsibilities is identified, assessed, and corrected in a timely manner or otherwise addressed at all levels of the organization. This enables the organization to actively address competence to support the achievement of the entity's objectives considering costs and benefits.

Plans and Prepares for Succession

201 Management continually identifies and assesses those performing functions that are deemed essential to achieving the entity's objectives. The importance of each role is determined by assessing what the impact would be if that role was temporarily or permanently unfilled. For instance, the chief executive officer and other members of senior management, strategic suppliers, and key channel partners are functions that typically require plans to be put in place to make sure those objectives can still be achieved, even in the absence of the individual filling the role.

202 Senior management and the board of directors develop contingency plans for assigning responsibilities important to internal control. In particular, succession plans for key executives are defined, and succession candidates are trained and coached for assuming the target role.

203 Succession planning is also undertaken when significant functions are delegated through contractual arrangements to outsourced service providers. Where an organization places considerable reliance on an external party and the organization has assessed the risk of that provider's processes or systems breaking down as having a direct impact on the entity's ability to achieve its objectives, some form of succession plan may be needed. Measures to provide for ongoing knowledge sharing and documentation ease the succession to a new provider when necessary.

Enforces Accountability

Principle 5: The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Points of Focus

204 The following points of focus may assist management in determining whether this principle is present and functioning:

- **Enforces Accountability through Structures, Authorities, and Responsibilities**—Management and the board of directors establish the mechanisms to communicate and hold individuals accountable for performance of internal control responsibilities across the organization and implement corrective action as necessary.
- **Establishes Performance Measures, Incentives, and Rewards**—Management and the board of directors establish performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity, reflecting appropriate dimensions of performance and expected standards of conduct, and considering the achievement of both short-term and longer-term objectives.
- **Evaluates Performance Measures, Incentives, and Rewards for Ongoing Relevance**—Management and the board of directors align incentives and rewards with the fulfillment of internal control responsibilities in the achievement of objectives.
- **Considers Excessive Pressures**—Management and the board of directors evaluate and adjust pressures associated with the achievement of objectives as they assign responsibilities, develop performance measures, and evaluate performance.
- **Evaluates Performance and Rewards or Disciplines Individuals**—Management and the board of directors evaluate performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence and provide rewards or exercise disciplinary action as appropriate.

Accountability for Internal Control

205 The board of directors ultimately holds the chief executive officer accountable for understanding the risks faced by the entity and establishing the requisite system of internal control to support the achievement of the entity's objectives. The CEO and senior management, in turn, are responsible for designing, implementing, conducting, and periodically assessing the structures, authorities, and responsibilities needed to establish accountability for internal control at all levels of the organization.

206 Accountability refers to the delegated ownership for the performance of internal control in the pursuit of objectives considering the risks faced by the entity. Outsourced service providers may be used to carry out responsibilities together with or on behalf of management, in which case management establishes the requisite levels of performance and oversight mechanisms and retains ultimate accountability for internal control. Management provides guidance to enable the understanding of risks faced by the entity, to communicate expectations of conduct of internal control responsibilities in support of the achievement of the entity's objectives, and to hold personnel accountable.

207 Accountability for internal control is demonstrated in each form of organizational structure used by the entity. For example, a manager whose responsibilities include upholding fair trade practices is accountable to the legal entity, operating unit, geography, or other existing structural entity to demonstrate an appropriate and effective control environment, risk assessment, control activities, information and communication, and monitoring to adhere to entity policy and support compliance with laws and regulations.

208 Accountability is interconnected with leadership, insofar as a strong tone at the top contributes to internal control responsibilities being understood, carried out, and continually strengthened across the entity. Tone helps to establish and enforce accountability, morale, and a common purpose through:

- Clarity of expectations from senior management and the board of directors, addressing issues such as integrity and ethics, conflict of interest, illegal or otherwise improper activities, and anticompetitive arrangements (e.g., a code of conduct is developed and communicated to all employees and outsourced service providers, and enforced)
- Guidance provided by management through its philosophy and operating style, as expressed in the form of state of mind, formality, persistence and other attitudes of management toward internal control (e.g., an entity that has been successful taking significant risks may have a different outlook on internal control than one that has faced harsh economic or regulatory consequences as a result of venturing into higher-risk areas)
- Control and information flow (e.g., communicating how decisions are made and, soliciting and acting on 360-degree feedback on performance)
- Upward and other communication channels for employees and outsourced service providers to feel comfortable reporting violations of ethical standards (e.g., anonymous or confidential communication channels are made available)

- Employee commitment toward collective objectives (e.g., alignment of individual goals and performance with the entity's objectives)
- Management's response to deviations from expected standards and behaviors (e.g., notices, terminations, and/or other corrective actions that ensue from failing to adhere to organizational standards, performance evaluation, and reward structures are commensurate with the achievement of the organization's objectives)

209 Accountability is driven by tone at the top and supported by the commitment to integrity and ethical values, competence, structure, processes, and technology, which collectively influence the control culture of the organization. Corrective action is taken as necessary to re-establish the necessary accountability for internal control.

Performance Measures, Incentives, and Rewards

210 Performance is greatly influenced by the extent to which individuals are held accountable and how they are rewarded.

211 Management and the board of directors establish performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity, considering the achievement of both short-term and longer-term objectives. Recognizing that rewarding future results in the present can yield unintended consequences, the organization establishes a combination of quantitative and qualitative performance measures balanced to reward successes and discipline behaviors as necessary in line with the range of objectives. Consider for example a company seeking to win customer loyalty with quality products. It engages its workforce in an effort to reduce production defect rates and aligns its performance measures, incentives, and rewards with both the operating unit's production goals and the expectations to comply with product safety and quality standards, workplace safety laws, customer loyalty programs, and accurate performance product data-reporting requirements.

212 Performance measures, incentives, and rewards support an effective system of internal control insofar as they are adapted to the entity's objectives and evolve dynamically with its needs. The following table illustrates key success measures and considerations for motivating, measuring and rewarding high performance.

Success Measures	Considerations
Clear Objectives	• Consider all levels of personnel to support the achievement of the entity's objectives. • Consider the multiple dimensions of expected conduct and performance of the organization, outsourced service providers and business partners (e.g., per service-level agreements), define objectives and related incentives and pressures.

Success Measures	Considerations
Defined Implications	• Communicate/reinforce the entity's objectives and how each area and level of the organization is expected to support the achievement of objectives. • Identify and discuss events that the market has rewarded in the past and those that the market has punished. • Communicate consequences (positive and negative) of not achieving or fully/partially achieving specific entity objectives.
Meaningful Metrics	• Define metrics to transform disparate data into meaningful information on performance. • Measure expected versus actual conduct and the impact of the deviations, both positive and negative. • Assess the expected impact on the entity's objectives.
Adjustment to Changes	• Adjust performance measures regularly based on a systematic and continual evaluation of the potential impacts of risks as they evolve over time, as well as the quantification of the associated rewards.

213 Incentives provide the motivation for management and other personnel to perform. Salary increases and bonuses are commonly used, but greater responsibility, visibility, recognition, and other forms of non-monetary reward are other effective incentives. Management consistently applies and regularly reviews the organization's measurement and reward structures to ensure that they do not encourage inappropriate conduct (e.g., lack of balance between revenue goals and other objectives key to the viability of the business can create conduct that is not in line with expected standards). Similarly, compensation and reward structures, including hiring and promotion structures, incorporate the review of historical conduct against expectations of ethical behavior. Individuals who do not adhere to the entity's standards of conduct are sanctioned and not promoted or otherwise rewarded.

214 Regardless of the form they take, incentives drive behavior. An entity that limits its focus to only increasing the bottom line may be more likely to experience unwanted behavior such as manipulation of the financial statements or accounting records, high-pressure sales tactics, negotiations directed at increasing quarterly sales or profit at any cost, or implicit offers of kickbacks.

215 Management and the board regularly evaluate the performance of individuals and teams in relation to defined performance measures, which include business performance factors as well as adherence and support for standards of conduct and demonstrated competence.

216 Performance measures are reviewed periodically for ongoing relevance and adequacy in relation to incentives and rewards. If necessary, internal or external factors are realigned to objectives and other expectations of management, personnel, and outside providers.

Pressures

217 Management and the board of directors establish goals and targets toward the achievement of objectives that by their nature create pressures within the organization. Pressures can also result from cyclical variations of certain activities, which organizations have the ability to influence by rebalancing workloads or increasing resource levels, as appropriate, to reduce the risk of employees "cutting corners" where it could be detrimental to the achievement of objectives.

218 These pressures which are further impacted by the internal or external environment can positively motivate individuals to meet expectations of conduct and performance, both in the short and long term. However, undue pressures can cause employees to fear the consequences of not achieving objectives and circumvent processes or engage in fraudulent activity or corruption.

219 Excessive pressures are most commonly associated with:

- Unrealistic performance targets, particularly for short-term results
- Conflicting objectives of different stakeholders
- Imbalance between rewards for short-term financial performance and those for long-term focused stakeholders, such as corporate sustainability goals

220 For example, pressure to generate sales levels that are not commensurate with market opportunities can lead sales managers to falsify numbers or engage in bribery or other illicit acts. Pressures to demonstrate the profitability of investments can cause traders to take off-strategy risks to cover incurred losses. Similarly, pressures to rush a product to market and generate revenues quickly may cause personnel to take shortcuts on product development or safety testing, which can be harmful to consumers or lead to poor acceptance or impaired reputation.

221 To align individual and business unit objectives to those of the entity, the organization considers how risks are taken and managed as a basis for compensation and other rewards. For example, as traders take risks on behalf of their clients and the organization, they are aware that their remuneration, advancement, and position can be boosted, reduced, or lost depending on their performance. Incentive structures that fail to adequately consider the risks associated with the business model can cause inappropriate behavior.

222 Other business changes, such as changes in strategy, organizational design, and acquisition/divestiture activity, also create pressures. Management and the board need to understand those pressures and balance them with appropriate messaging and incentives/rewards. Management and the board set and adjust as appropriate the pressures on incentives and rewards when assigning responsibilities, designing performance measures, and evaluating performance. It is management's responsibility to guide those to whom they have delegated authority to make appropriate decisions in the course of doing business. For example, organizations often view financial performance, development of competencies, and timely and accurate reporting to stakeholders as their most critical objectives for the viability of the business. They also expect management,

other personnel, and outsourced service providers and business partners to preserve at all times the quality of products or services delivered, safety of personnel performing its functions, and other factors that could create a moral hazard or damage the entity's reputation.

Performance Evaluation and Reward

223 Just as performance objectives are cascaded down from the board of directors to the chief executive officer, senior management, and other personnel, performance evaluation is conducted at each of these levels. The board of directors evaluates the performance of the CEO, who in turn evaluates that of the senior management team, and so on. At each level, adherence to standards of conduct and expected levels of competence is evaluated, and rewards are allocated or disciplinary action is exercised as appropriate. Rewards may be in the form of money, equity, recognition, or career progression. The results of these evaluations are communicated and acted upon with rewards or sanctions as applicable to influence desired behavior.

224 Compensation policies and practices are based on the compensation philosophy of the organization, which considers the competitive positioning it seeks to achieve (methods and levels of incentive and compensation to attract the highest caliber talent needed to be superior to offers from industry peers). Compensation and other rewards are awarded on the basis of performance evaluation, competencies, and skill acquisition, as well as available market pricing information, with the goal of retaining high performers and encouraging attrition of lower-end performers. Human resources manages the process of obtaining, processing, and communicating the relevant information to appropriate levels of management and other personnel.

225 Performance is measured in relation to the achievement of objectives and the ability to manage within risk tolerance levels considering both the short and long term. As such, it considers both historical (retrospective) and forward-looking (prospective) risks.

6. Risk Assessment

Chapter Summary

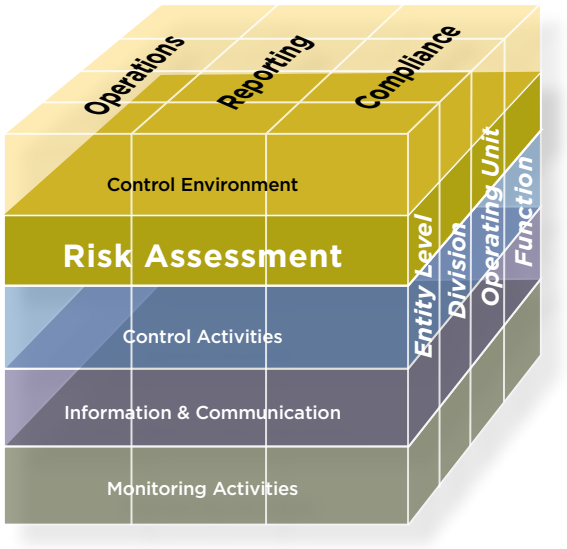
226 Every entity faces a variety of risks from external and internal sources. Risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives. Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Risks to the achievement of these objectives from across the entity are considered relative to established risk tolerances. Thus, risk assessment forms the basis for determining how risks will be managed. A precondition to risk assessment is the establishment of objectives, linked at different levels of the entity. Management specifies objectives within categories relating to operations, reporting, and compliance with sufficient clarity to be able to identify and analyze risks to those objectives. Management also considers the suitability of the objectives for the entity. Risk assessment also requires management to consider the impact of possible changes in the external environment and within its own business model that may render internal control ineffective.

Principles relating to the Risk Assessment component

6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.
9. The organization identifies and assesses changes that could significantly impact the system of internal control.

Introduction

227 All entities, regardless of size, structure, nature, or industry, encounter risks at all levels. Risk is defined in the Framework as the possibility that an event will occur and adversely affect the achievement of objectives.



228 The use of the term "adversely" in this definition does not ignore positive variances relating to an event or series of events. Large positive variances may still create adverse impacts to objectives. For instance, consider a company that forecasts sales of 1,000 units and sets production schedules to achieve this expected demand. Management considers the possibility that actual orders will exceed this forecast. Actual orders of 1,500 units would likely not impact the sales objectives but might adversely impact production costs (through incremental overtime needed to meet increased volumes) or customer satisfaction targets (through increased back orders and wait times). Consequently, selling more units than planned may adversely impact objectives other than the sales objective.

229 As part of the process of identifying and assessing risks, an organization may also identify opportunities, which are the possibility that an event will occur and positively affect the achievement of objectives. These opportunities are important to capture and to communicate to the objective-setting processes. For instance, in the above example, management would channel new sales opportunities to the objective-setting processes. However, identifying and assessing potential opportunities such as new sales opportunities is not a part of internal control.

230 Risks affect an entity's ability to succeed, compete within its industry, maintain its financial strength and positive reputation, and maintain the overall quality of its products, services, and people. There is no practical way to reduce risk to zero. Indeed, the decision to be in business incurs risk. Management must determine how much risk is to be prudently accepted, strive to maintain risk within these levels, and understand how much tolerance it has for exceeding its target risk levels.

231 Risk often increases when objectives differ from past performance and when management implements change. An entity often does not set explicit objectives when it considers its performance to be acceptable. For example, an entity might view its historical service to customers as acceptable and therefore not set specific goals on maintaining current levels of service. However, as part of the risk assessment process, the organization does need to have a common understanding of entity-level objectives relevant to operations, reporting, and compliance and how those cascade into the organization.

Risk Tolerance

232 Risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. Operating within risk tolerance provides management with greater confidence that the entity will achieve its objectives. Risk tolerance may be expressed in different ways to suit each category of objectives. For instance, when considering financial reporting, risk tolerance is typically expressed in terms of materiality,[7] whereas for compliance and operations, risk tolerance is often expressed in terms of the acceptable level of variation in performance.

233 Risk tolerance is normally determined as part of the objective-setting process, and as with setting objectives, setting tolerance levels is a precondition for determining risk responses and related control activities. Management may exercise significant discretion in setting risk tolerance and managing risks when there are no external requirements. However, when there are external requirements, such as those relating to external reporting and compliance objectives, management considers risk tolerance within the context of established laws, rules, regulations, and external standards.

234 As well, senior management considers the relative importance of the competing objectives and differing priorities for pursuing these objectives. For instance, a chief operating officer may view operations objectives as requiring a higher level of precision than materiality considerations in reporting objectives, and vice versa for the chief financial officer. However, it would be problematic for public companies to overemphasize operational objectives to an extent that adversely impacts the reliability of financial reporting. These views are considered as part of the strategic-planning and objective-setting process with tolerances set accordingly. This kind of decision may also impact the level of resources allocated to pursuing the achievement of those respective objectives.

235 Performance measures are used to help an entity operate within established risk tolerance. Risk tolerance is often best measured in the same unit as the related objectives. For example, an entity:

- Targets on-time delivery at 98%, with acceptable variation in the range of 97% to 100%
- Targets training with 90% of those taking the training attaining a pass rate, but accepts that only 75% of those taking the test may pass
- Expects staff to respond to all customer complaints within twenty-four hours, but accepts that up to 10% of complaints may receive a response within thirty-six hours

7 Regulators and standard-setting bodies define the term "materiality." Management develops an understanding of materiality as defined by laws, rules, and standards when applying the Framework in the context of such laws, rules, and standards.

Specifies Suitable Objectives

Principle 6: The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

236 A precondition to risk assessment is the establishment of objectives, linked at various levels of the entity. These objectives align with and support the entity in the pursuit of its strategic direction. While setting strategies and objectives is not part of the internal control process, objectives form the basis on which risk assessment approaches are implemented and performed and subsequent control activities are established. As part of internal control, management specifies objectives and groups them within broad categories at all levels of the entity, relating to operations, reporting, and compliance. The grouping of objectives within these categories allows for the risks to the achievement of those objectives to be identified and assessed.

237 In considering the suitability of objectives, management may consider such matters as:

- Alignment between established objectives and strategic priorities
- Articulation of risk tolerances for objectives
- Alignment between established objectives and established laws, rules, regulations, and standards applicable to the entity
- Articulation of objectives using terms that are specific, measurable or observable, attainable, relevant, and time-bound
- Cascading of objectives across the entity and it subunits
- Alignment of objectives to other circumstances that require specific focus by the entity
- Approval objectives within the objective-setting process

238 Where objectives within these categories are unclear, where it is unclear how these objectives support the strategic direction, or where there are concerns that the objectives are not suitable based on the facts, circumstances, and established laws, rules, regulations, and standards applicable to the entity, management communicates this concern for input to the strategy-setting and objective-setting process.

Operations Objectives

Points of Focus

239 The following points of focus may assist management in determining whether this principle is present and functioning as it relates to operations objectives:

- **Reflects Management's Choices**—Operations objectives reflect management's choices about structure, industry considerations, and performance of the entity.
- **Considers Tolerances for Risk**—Management considers the acceptable levels of variation relative to the achievement of operations objectives.
- **Includes Operations and Financial Performance Goals**—The organization reflects the desired level of operations and financial performance for the entity within operations objectives.
- **Forms a Basis for Committing of Resources**—Management uses operations objectives as a basis for allocating resources needed to attain desired operations and financial performance.

Management Choices

240 Operations objectives reflect management choices within the particular business, industry, and economic environments in which the entity functions. For instance, a municipal government sets out several operations objectives, each supported by initiatives and criteria. Among its objectives are to, for example:

- Implement five public engagement activities for greenhouse gas reductions within the next twelve months
- Increase seatbelt use by 30%, reduce speeding by 10% in general and 20% in school zones, and reduce intersection encroachment by 25%
- Implement water rates relative to industrial and residential consumption patterns within five years

241 A for-profit entity may set operations objectives that focus on the efficient uses of resources. For instance, a larger retailer has among its objectives to:

- Provide customers with a broad range of merchandise at prices consistently lower than its competitors
- Increase inventory turnover ratio to twelve times per year within the next two quarters
- Lower its CO^2 emissions by 5% and reduce and recycle packaging material by 10% over the next year

242 As part of operations objectives, management also specifies risk tolerance set during the objective-setting process. For operations objectives, risk tolerance may be expressed in relation to the acceptable level of variation relative to the objective.

Goals and Resources

243 A clear set of operations objectives provides a clear focus on which the entity will commit substantial resources needed to attain desired performance goals. These include goals relating to financial performance, which pertain to all types of entities. A for-profit entity may focus on revenue, profitability, liquidity, or some other measure, while a not-for-profit or governmental agency may have less financial emphasis overall, but still pursue goals relating to revenue, liquidity, and spending. If an entity's operations objectives are not clear or well conceived, its resources may be misdirected.

Reporting Objectives

244 Reporting objectives pertain to the preparation of reports that encompass reliability, timeliness, transparency, or other terms as set forth by regulators, standard-setting bodies, or by the entity's policies. This category includes external financial reporting, external non-financial reporting, internal financial reporting, and internal non-financial reporting. External reporting objectives are driven primarily by laws, rules, regulations, and standards established by governments, regulators, standard-setting bodies, and accounting bodies. Internal reporting objectives are driven by the entity's strategic directions, and by reporting requirements and expectations established by management and the board of directors.

External Financial Reporting Objectives

Points of Focus

245 The following points of focus may assist management in determining whether this principle is present and functioning as it relates to external financial reporting objectives:

- **Complies with Applicable Accounting Standards**—Financial reporting objectives are consistent with accounting principles suitable and available for that entity. The accounting principles selected are appropriate in the circumstances.
- **Considers Materiality**—Management considers materiality in financial statement presentation.
- **Reflects Entity Activities**—External reporting reflects the underlying transactions and events to show qualitative characteristics and assertions.

Complies with Accounting Standards

246 Entities need to achieve financial reporting objectives to meet external obligations. Published financial statements and financial information are necessary for accessing capital markets and may be critical to the awarding of contracts or to dealing with suppliers. Investors, analysts, and creditors may use financial statements and other

financial information to assess the entity's performance and to compare it with peers and alternative investments.

247 Financial reporting objectives are consistent with accounting principles suitable and available for that entity and appropriate in the circumstances. External financial reporting objectives address the preparation of external financial statements, including financial statements, for external purposes, and other forms of external financial reporting derived from an entity's financial or management accounting books and records.

- Financial statements for external purposes are prepared in accordance with applicable accounting standards, rules, and regulations. These financial statements include annual and interim financial statements, condensed financial statements, and selected financial information derived from such statements. These statements may, for instance, be publicly filed with a regulator, distributed through annual meetings, posted to an entity's website, or distributed through other electronic media.
- Other financial statements/reports may be prepared in accordance with other comprehensive basis of accounting and are typically driven by taxing authorities, governmental agencies, or by requirements established through contracts and agreements. Other external financial statements/reports may be distributed to specified external users (e.g., reporting to a bank on financial covenants established in a loan agreement, to a taxing authority in connection with filing tax returns, to a funding agency by a not-for-profit entity where such statements are not made public).
- Other external financial reporting derived from an entity's financial and management accounting books and records rather than from financial statements for external purposes may include earnings releases, selected financial information posted to an entity's website, and selected amounts reported in regulatory filings. External financial reporting objectives relating to such other financial information may not be driven directly by standard setters and regulators, but are typically expected by stakeholders to align with such standards and regulations.

Qualitative Characteristics

248 External financial reporting reflects transactions and events to show the qualitative characteristics and assertions that underlie financial statements established by the respective accounting standard setters. There are many sources of such characteristics and assertions relating to financial reporting.

249 External financial statements may be considered in terms of *fundamental characteristics* and *enhancing characteristics*.[8,9]

8 Derived from International Financial Reporting Standards.

9 Some jurisdictions may describe financial statement assertions using terms such as "existence or occurrence," "completeness, valuation or allocation," "rights and obligations," and "presentation and disclosure."

250 Fundamental characteristics refer to relevance and faithful representation, as follows:

- *Relevance*—information that is capable of making a difference in user decisions
- *Faithful Representation*—information that is complete, neutral, and free from error

251 Enhancing characteristics refer to comparability, verifiability, timeliness, and understandability, as follows:

- *Comparability*—information that can be compared with similar information about other entities and with similar information about the same entity for another period or another date
- *Verifiability*—different knowledgeable and independent observers reaching consensus, although not necessarily complete agreement, that a particular depiction is a faithful representation
- *Timeliness*—having information available to decision-makers in time to be of use
- *Understandability*—information that is classified, characterized, and presented clearly and concisely

252 Inherent in relevance is the concept of "financial statement materiality." Materiality sets the threshold for determining whether a financial amount is relevant. Information is material if its omission or misstatement could influence the decision of users taken on the basis of the financial reporting. Materiality depends on the size of the item or error judged in the particular circumstances of its omission or misstatement. With external financial reporting, materiality reflects the required level of precision and accuracy suitable for external users' needs and presents the underlying entity activities, transactions, and events within the range of acceptable limits.

253 Reliability is another frequently used qualitative characteristic associated with external financial reporting objectives. Reliability involves preparing external financial statements that are free of material error and bias. Reliability is also necessary for the information to faithfully represent the transactions or other events it purports to represent. External reporting also reflects the required level of precision and accuracy suitable for internal needs and the underlying entity activities, presenting transactions, and events within a range of acceptable limits.

254 The qualitative characteristics noted above are applied along with suitable accounting standards and financial statement assertions. These assertions typically fall into the categories relating to:

- Classes of transactions and events for the period
- Account balances at the period end
- Presentation and disclosure[10]

10 Derived from International Auditing and Assurance Standards Board (IAASB) International Standards on Auditing 315.

External Non-Financial Reporting Objectives

Points of Focus

255 The following points of focus may assist management in determining whether this principle is present and functioning as it relates to external non-financial reporting objectives:

- **Complies with Externally Established Standards and Frameworks**—Management establishes objectives consistent with laws and regulations, or standards and frameworks of recognized external organizations.
- **Considers the Required Level of Precision**—Management reflects the required level of precision and accuracy suitable for user needs and as based on criteria established by third parties in non-financial reporting.
- **Reflects Entity Activities**—External reporting reflects the underlying transactions and events within a range of acceptable limits.

Complies with Standards and Frameworks

256 Management may also report information externally consistent with non-financial external standards or frameworks. For example, where management seeks to manage its impact on sustainable development, it may prepare and publish a sustainability report that provides information about economic, environmental, and social performance. Another entity may apply chain-of-custody standards through which its products are distributed from their origin in the forest to their end use. The entity attains an annual certification that demonstrates its responsible production and consumption of forest products and publicly reports this information.

Considers Precision and Reflects Activities

257 Non-financial reporting, as with financial reporting:

- Classifies and summarizes information in a reasonable manner and at the appropriate level of detail so that it is neither too detailed nor too condensed
- Reflects the underlying entity activities
- Presents transactions and events within the required level of precision and accuracy suitable for user needs
- Uses criteria established by the third parties and as set out in external standards or frameworks, as appropriate

Internal Reporting Objectives

Points of Focus

258 The following points of focus may assist management in determining whether this principle is present and functioning as it relates to internal reporting objectives:

- **Reflects Management's Choices**—Internal reporting provides management with accurate and complete information regarding management's choices and information needed in managing the entity.
- **Considers the Required Level of Precision**—Management reflects the required level of precision and accuracy suitable for user needs in non-financial reporting objectives and materiality within financial reporting objectives.
- **Reflects Entity Activities**—Internal reporting reflects the underlying transactions and events within a range of acceptable limits.

Management Choices

259 Reliable internal reporting, including balanced scorecards and performance dashboards, provides management with accurate and complete information needed to manage the organization. It supports management's decision making and monitoring of the entity's activities and performance. Examples of internal reports include results of marketing programs, daily sales flash reports, production quality, and employee and customer satisfaction results. Internal reporting objectives are based on preferences, judgment, and management style.

260 Internal reporting objectives vary among entities because different organizations have different goals, strategic directions, and levels of risk tolerance. As with external reporting, internal reporting reflects the required level of precision and accuracy suitable for internal needs and the underlying entity activities, presenting transactions and events within a range of acceptable limits.

261 Many organizations will apply external standards to assist in managing their operations. Such standards may relate to the control over technology, human resource management, or records management. However, as standards that apply to external reporting may not apply to internal reporting, management may choose to set different levels of acceptable variation for external and internal reporting.

262 As with other types of reporting, internal reporting:

- Uses criteria established by the third parties and as set out in external standards or frameworks, as appropriate
- Classifies and summarizes information in a reasonable manner and at the appropriate level of detail so that it is neither too detailed nor too condensed
- Reflects the underlying entity activities
- Presents transactions and events within the required level of precision and accuracy suitable for user needs

Compliance Objectives

Points of Focus

263 The following points of focus may assist management in determining whether this principle is present and functioning as it relates to compliance objectives:

- **Reflects External Laws and Regulations**—Laws and regulations establish minimum standards of conduct which the entity integrates into compliance objectives.
- **Considers Tolerances for Risk**—Management considers the acceptable levels of variation relative to the achievement of compliance objectives.

Minimum Standards of Conduct

264 Laws and regulations establish minimum standards of conduct that the entity integrates into its compliance objectives. For example, occupational safety and health regulations might cause an entity to define its objective as "package and label all chemicals in accordance with regulations." Policies and procedures would then deal with communications programs, site inspections, and training relating to the entity's compliance objectives. And, similar to external reporting objectives, management considers the acceptable levels of variation in performance within the context of complying with laws and regulations. Such laws and regulations may cause management to set lower levels of acceptable variation to remain in compliance with those laws and regulations.

265 Entities must conduct their activities, and often take specific actions, in accordance with applicable laws and regulations. As part of specifying compliance objectives, the organization needs to understand which laws and regulations apply across the entity. Many laws and regulations are generally well known, such as those relating to reporting on anti-bribery, fair labor practices, and environmental compliance, but others may not be as well known to the organization, such as those that apply to operations in a remote foreign territory.

266 Many laws and regulations depend on external factors and tend to be similar across all entities in some cases and across an industry in others. These requirements may relate, for example, to markets, pricing, taxes, the environment, employee welfare, or international trade. Many entities will establish objectives such as:

- Preventing and detecting criminal conduct and other wrongdoing
- Preparing and filing tax returns prior to the filing deadlines and in accordance with regulatory requirements
- Labeling nutritional information on food packaging in accordance with applicable guidelines
- Operating a vehicle fleet within maximum emission control requirements

Identifies and Analyzes Risk

Principle 7: The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

Points of Focus

267 The following points of focus may assist management in determining whether this principle is present and functioning:

- **Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels**—The organization identifies and assesses risks at the entity, subsidiary, division, operating unit, and functional levels relevant to the achievement of objectives.
- **Analyzes Internal and External Factors**—Risk identification considers both internal and external factors and their impact on the achievement of objectives.
- **Involves Appropriate Levels of Management**—The organization puts into place effective risk assessment mechanisms that involve appropriate levels of management.
- **Estimates Significance of Risks Identified**—Identified risks are analyzed through a process that includes estimating the potential significance of the risk.
- **Determines How to Respond to Risks**—Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.

268 Identifying and analyzing risk is an ongoing iterative process conducted to enhance the entity's ability to achieve its objectives. Although an entity might not explicitly state all objectives, this does not mean that an implied objective is without either internal or external risk. Regardless of whether an objective is stated or implied, an entity's risk assessment process should consider risks that may occur. This process is supported by a variety of activities, techniques, and mechanisms, each relevant to overall risk assessment. Management develops and implements controls relating to the conduct of such activities.

269 Management considers risks at all levels of the entity and takes the necessary actions to respond. An entity's assessment considers factors that influence the severity, velocity, and persistence of the risk, likelihood of the loss of assets, and the related impact on operations, reporting, and compliance activities. The entity also needs to understand its tolerance for accepting risks and its ability to operate within those risk levels.

Risk Identification

270 Risk identification must be comprehensive. It should consider all significant interactions—of goods, services, and information—internal to an entity and between the entity and its relevant business partners and outsourced service providers. These entities can include potential and existing suppliers, investors, creditors, shareholders, employees, customers, buyers, intermediaries, and competitors, as well as public bodies and news media. In addition, the organization should consider risks emanating from external factors such as new or amended laws and regulations, environmental issues, or potential natural events.

271 Further, risks related primarily to one category of objectives may impact objectives in other categories. For instance, a risk relating primarily to an operations objective for the timely production and delivery of a company's product may also impact financial reporting if the company's sales contract contains penalties for late shipments. In those instances where an organization is considering risks relating primarily to one category of objectives, for instance financial reporting, the risk assessment process may need to consider objectives in other categories that can also impact financial reporting objectives.

272 Risk identification is an iterative process and is often integrated with the planning process. However, it may be useful to take a fresh look at the identified risks, and not merely default to making an inventory of risks as noted in the previous review. The focus is on identifying all risks that potentially impact the achievement of objectives as well as on emerging risks—those risks that are increasingly relevant and important to the entity and that may be addressed by scanning and analyzing relevant risk factors, as remote as they may seem.

Considers Entity and Subunits

273 Risk identification considers risks at various levels of the organizational structure, including the overall entity and its subunits, including processes such as sales, human resources, marketing, production, and purchasing. Entity-level risk identification is typically conducted at a relatively high level and, generally, does not include assessing transaction-level risks. Conversely, the identification of risks at a process level is inherently more detailed and would include transaction-level risks.

274 In addition, risk assessment considers risks originating in outsourced service providers, key suppliers, and channel partners that directly or indirectly impact the entity's achievement of objectives.

Internal and External Factors

275 Management considers risks in relation to internal and external factors. Risk is dynamic; therefore, to determine the frequency of its risk assessment process, management generally considers the rate of change in risks to the achievement of objectives, other operational priorities, and cost. Typically, the process is a combination of ongoing and periodic risk assessments. If the rate of change relating to an objective or internal and external factors increases, it is useful to accelerate the frequency of assessing the related risks or assess the risk on a real-time basis.

Entity-Level Risks

276 Risks at the entity level can arise from external or internal factors. External factors may include:

- *Economic*—Changes that can impact financing, capital availability, and barriers to competitive entry
- *Natural Environment*—Natural or human-caused catastrophes or ongoing climate change that can lead to changes in operations, reduced availability of raw materials, or loss of information systems, highlighting the need for contingency planning
- *Regulatory*—A new financial reporting standard that can require different or additional reporting by a legal entity, management operating model, or line of business; a new anti-trust law or regulation that can force changes in operating or reporting policies and strategies
- *Foreign Operations*—A change in the government of a foreign country of operation that can result in new laws and regulations or altered tax regimes
- *Social*—Changing customer needs or expectations that can affect product development, production process, customer service, pricing, or warranties
- *Technological*—Developments that can affect the availability and use of data, infrastructure costs, and the demand for technology-based services

277 Internal factors include:

- *Infrastructure*—Decisions on the use of capital resources that can affect operations and the ongoing availability of infrastructure
- *Management Structure*—A change in management responsibilities that can affect the way certain controls are effected
- *Personnel*—The quality of personnel hired and methods of training and motivation that can influence the level of control consciousness within the entity; expiration of labor agreements that can affect the availability of staff
- *Access to Assets*—The nature of the entity's activities and employee accessibility to assets that can contribute to misappropriation of resources
- *Technology*—A disruption in information systems processing that can adversely affect the entity's operations

278 Identifying external and internal factors that contribute to risk at an entity level is critical to comprehensive risk assessment. Once the major factors have been identified, management can then consider their relevance and significance and, where possible, link these factors to specific risks and activities.

279 For example, an importer of apparel and footwear established an entity-level objective of becoming an industry leader in high-quality fashion merchandise. The entity considered general risks such as the impact of deterioration in economic conditions,

market acceptance of products, new competitors in the entity's market, and changes in environmental or regulatory laws and regulations. In addition, the entity considered risks at the entity level such as:

- Supply sources, including the quality, quantity, and stability of foreign manufacturers
- Exposures to fluctuations in the value of foreign currencies
- Timeliness of receiving shipments and delays in customs inspections
- Availability and reliability of shipping companies and costs
- Likelihood of international hostilities and trade embargoes
- Pressures from customers and investors to boycott doing business in a foreign country whose government adopts unacceptable policies
- Expectations from consumers or local stakeholders toward use of natural resources

Transaction-Level Risks

280 Risks are identified at the transaction level within subsidiaries, divisions, operating units, or functions. Dealing with risks at this level helps focus on the achievement of objectives and/or sub-objectives that have cascaded down from the entity-level objectives. Successfully assessing risk at the transaction level also contributes to maintaining acceptable levels at the entity level.

281 In most instances, many different risks can be identified. In a procurement process, for example, an entity may have an objective related to maintaining adequate raw materials inventory. The risks to not achieving this objective might include suppliers providing materials that do not meet specifications or are not delivered in needed quantities, on time, or at acceptable prices. These risks might affect entity-level objectives pertaining to the way specifications for purchased goods are communicated to vendors, the use and appropriateness of production forecasts, identification of alternative supply sources, and negotiation practices.

282 Potential causes of failing to achieve an objective range from the obvious to the obscure. Certainly, readily apparent risks that significantly affect the entity should be identified. To avoid overlooking relevant risks, this identification is best made apart from assessing the likelihood of the risk occurring. There are, however, practical limitations to the identification process, and often it is difficult to determine where to draw the line. For example, it may not make sense to conduct a detailed assessment of the risk of a meteor falling from space onto an entity's production facility, while it may be reasonable for a facility located near an airport to consider in some detail the risk of an airplane crash.

Risk Analysis

283 After risks have been identified at both the entity level and the transaction level, a risk analysis needs to be performed. The methodology for analyzing risks can vary, largely because many risks are difficult to quantify. Nonetheless, the process—which may be more or less formal—usually includes assessing the likelihood of the risk occurring and estimating its impact. In addition, the process could consider other criteria to the extent management deems necessary.

Levels of Management

284 As with other processes within internal control, responsibility and accountability for risk identification and analysis processes reside with management at the overall entity and its subunits. The organization puts into place effective risk assessment mechanisms that involve appropriate levels of management with expertise.

Significance of Risk

285 As part of risk analysis, the organization assesses the significance of risks to the achievement of objectives and sub-objectives. Organizations may assess significance using criteria such as:

- Likelihood of risk occurring and impact
- Velocity or speed to impact upon occurrence of the risk
- Persistence or duration of time of impact after occurrence of the risk

286 "Likelihood" and "impact" are commonly used terms, although some entities use instead "probability," "severity," "seriousness," or "consequence." "Likelihood" represents the possibility that a given event will occur, while "impact" represents its effect. Sometimes the words take on more specific meaning, with "likelihood" indicating the possibility that a given risk will occur in qualitative terms such as "high," "medium," and "low," and "probability" indicating a quantitative measure such as a percentage, frequency of occurrence, or other numerical metric.

287 Risk velocity refers to the pace with which the entity is expected to experience the impact of the risk. For instance, a manufacturer of consumer electronics may be concerned about changing customer preferences and compliance with radio frequency energy limits. Failing to manage either of these risks may result in significant erosion in the entity's value, even to the point of being put out of business. In this instance, changes in regulatory requirements develop much more slowly than do changes in customer preferences.

288 Management often uses performance measures to determine the extent to which objectives are being achieved, and normally uses the same or a congruent unit of measure when considering the potential impact of a risk on the achievement of a specified objective. An entity, for example, with an objective of maintaining a specified level of customer service will have devised a rating or other measure for that objective—such as a customer satisfaction index, number of complaints, or measure of repeat business. When assessing the impact of a risk that might affect customer service—such as the possibility that the entity's website might be unavailable for a time period—impact is best determined using the same measures.

289 A risk that does not have a significant impact on the entity and that is unlikely to occur generally does not require a detailed risk response. A risk with a higher likelihood of occurrence and/or the potential of a significant impact, on the other hand, typically results in considerable attention. But even those risks with a potentially high impact that have a low likelihood will be considered, avoiding the notion that such risks "couldn't happen here," as even low likelihood risks can occur. The importance of understanding risks assessed as having a low likelihood is greater when the potential impact of the risk might persist over a longer period of time. For instance, the long-term impact on the entity from environmental damage caused by the entity's actions may be viewed much differently than the long-term impact of losing technology processing in a manufacturing plant for several days.

290 Estimates of significance of the risk often are determined by using data from past events, which provide a more objective basis than entirely subjective estimates. Internally generated data based on an entity's own experience may be more relevant and provide better results than data from external sources. Even in these circumstances, however, external data can be useful as a checkpoint or to enhance the analysis. For example, a company's management assessing the risk of production stoppages because of equipment failure looks first at frequency and impact of previous failures of its own manufacturing equipment. It then supplements that data with industry benchmarks. This allows a more precise estimate of likelihood and impact of failure, enabling more effective preventive maintenance scheduling. Note, too, that using data from past events can provide incomplete conclusions where events occur infrequently.

291 In addition, management may wish to assess risks using a time horizon consistent with the time horizon of the related objectives. Because the objectives of many entities focus on the short- to mid-term, management analyzes risks associated with those time frames. However, some objectives extend to the longer term, and management must not ignore those risks that might be further into the future.

Inherent and Residual Risk

292 Management considers both inherent and residual risk. Inherent risk is the risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact. Residual risk is the risk that remains after management's response to inherent risk. Risk analysis is applied first to inherent risk. Once risk responses have been developed, as discussed below, management then considers residual risk. Assessing inherent risk in addition to residual risk can assist the organization in understanding the extent of risk responses needed. However, management may choose to focus primarily on residual risk.

Risk Response

293 Once the potential significance of risks has been assessed, management considers how the risk should be managed. This involves applying judgment based on assumptions about the risk and reasonable analysis of costs associated with reducing the level of risk. The response need not necessarily result in the least amount of residual risk. But where a risk response would result in residual risk exceeding levels acceptable to management and the board, management revisits and revises the response or, in certain

instances, reconsiders the established risk tolerance. Accordingly, the balancing of risk and risk tolerance may be iterative.

294 Risk responses fall within the following categories:

- *Acceptance*—No action is taken to affect risk likelihood or impact.
- *Avoidance*—Exiting the activities giving rise to risk; may involve exiting a product line, declining expansion to a new geographical market, or selling a division.
- *Reduction*—Action is taken to reduce risk likelihood or impact, or both; typically involves any of myriad everyday business decisions.
- *Sharing*—Reducing risk likelihood or impact by transferring or otherwise sharing a portion of the risk; common techniques include purchasing insurance products, forming joint ventures, engaging in hedging transactions, or outsourcing an activity.

295 In considering risk response, management should consider:

- The potential effect on risk significance and which response options align with the entity's risk tolerance
- Requisite segregation of duties to enable the response to achieve the intended reduction in significance
- Costs versus benefits of potential responses

Evaluating Risk Response Options

296 In evaluating response options, management considers significance, including the effect on both likelihood and impact of the risk, recognizing that a response might affect them differently. For example, consider a company with a data center located in a region with heavy storm activity. It establishes a business continuity plan, which, while having no effect on the likelihood of a storm occurring, mitigates the impact of building damage or personnel being unable to get to work should a storm occur. On the other hand, the choice to move the computer center to another region will not reduce the impact of a comparable storm, but could reduce the likelihood of a similar storm occurring near that new location.

297 Resources always have constraints, and entities must consider the relative costs and benefits of alternative risk response options. Before installing additional procedures, management should consider carefully whether existing ones may be suitable for addressing identified risks. Because procedures may satisfy multiple objectives, management may discover that additional actions are not warranted or that existing procedures may be sufficient or simply need to be performed to a higher standard.

Selected Responses

298 There is a distinction between risk assessment, which is part of internal control, and the choice of specific risk responses and the related plans, programs, or other actions, which are part of the management process and not internal controls. Internal control does not encompass ensuring that the optimal risk response is chosen. For instance, the management of one entity may choose to share technology risk by outsourcing certain aspects of its technology processing with an entity experienced in that field (recognizing that this may also introduce new risks to the organization), while another entity may choose to retain its technology processing and develop general controls over activities for managing related technology risks. Neither of these choices should be viewed as right or wrong, as both can be effective at managing technology risks. But where a risk response would result in the residual risk exceeding risk tolerances for any category of objectives, management revisits and revises the response accordingly.

299 Once management has chosen to reduce or share a risk, then it can determine actions to respond to the risk and select and develop associated control activities. The nature and extent of the risk response and any associated control activities will depend, at least in part, on the desired level of risk mitigation (which is the focus of Chapter 7). In some instances, management may select a response that requires action within another component of internal control—for instance enhancing a part of the control environment.

300 Typically, control activities are not needed when an entity chooses to either accept or avoid a specific risk. For instance, a mining company with significant commodity price risk may decide to accept the risk as it believes that investors are aware of and accept price risk exposure. In this case, management would not implement control activities relating to commodity price exposures, but would likely implement control activities relating to other external financial reporting assertions, including completeness and valuation. There may, however, be instances where the organization decides to avoid a risk, and chooses to develop control activities in order to avoid that risk. For instance, to avoid concerns over possible fair trade practices, an organization may implement control activities barring purchasing from certain entities.

301 Management may also need to review the level of risk in light of changes that make it no longer desirable to accept that risk, as the risk now exceeds the organization's risk tolerance. When management chooses not to assess a risk or does not identify a risk, it is tantamount to accepting the risk without considering potential changes in the related level of risk and whether that risk remains within its risk tolerance.

Assesses Fraud Risk

Principle 8: The organization considers the potential for fraud in assessing risks to the achievement of objectives.

Points of Focus

302 The following points of focus may assist management in determining whether this principle is present and functioning:

- **Considers Various Types of Fraud**—The assessment of fraud considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.
- **Assesses Incentive and Pressures**—The assessment of fraud risk considers incentives and pressures.
- **Assesses Opportunities**—The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering of the entity's reporting records, or committing other inappropriate acts.
- **Assesses Attitudes and Rationalizations**—The assessment of fraud risk considers how management and other personnel might engage in or justify inappropriate actions.

Types of Fraud

303 Risk assessment includes management's assessment of the risks relating to the fraudulent reporting and safeguarding of the entity's assets. In addition, management considers possible acts of corruption, both by entity personnel and by outsourced service providers directly impacting the entity's ability to achieve its objectives.

304 The actions being conducted as part of applying this principle link closely to the preceding principle (see Identifies and Analyzes Risks), which assesses risks based on the presumption that the entity's expected standards of ethical conduct are adhered to by management, other personnel, and outsourced service providers. This principle, Assesses Fraud Risk, assesses risk in a different context, when an individual's actions may not align with the expected standards of conduct. Responses to risks identified as part of this principle fall within the same categories noted above (accept, avoid, reduce, and share). And, as above, the selection of specific risk responses to address fraud risks is a management decision and not part of internal control.

Fraudulent Reporting

305 Fraudulent reporting can occur when an entity's reports are wilfully prepared with misstatements or omissions. These events may occur through unauthorized receipts or expenditures, financial misconduct, or other disclosure irregularities. A system of

internal control over external financial reporting is designed and implemented to prevent or detect, in a timely manner, any material misstatement within the financial statements due to error or fraud.

306 When assessing risks to the achievement of external financial reporting objectives, organizations typically consider the potential for fraud in the following areas:

- *Fraudulent External Financial Reporting*—An intentional act designed to deceive users of external financial reports and that results in a material misstatement in such financial reports
- *Misappropriation of Assets*—Theft of the entity's assets where the effect causes a material misstatement in the external financial reports
- *Illegal Acts*—Violations of laws or governmental regulations that could have a material direct or indirect impact on the external financial report.

307 As part of the risk assessment process, the entity should identify the various ways that fraudulent reporting can occur, considering:

- Degree of estimates and judgments in external reporting
- Fraud schemes and scenarios common to the industry sectors and markets in which the entity operates
- Geographic regions where the entity does business
- Incentives that may motivate fraudulent behavior
- Nature of technology
- Unusual or complex transactions subject to significant management influence
- Vulnerability to management override and potential schemes to circumvent existing control activities

308 There may be instances where the organization is not able to directly manage the information captured for financial reporting, yet is expected to have controls within the entity that identify, analyze, and respond to that particular risk. For instance, management of a software vendor may not be able to prevent personnel within an on-line retailer from underreporting sales numbers to reduce payments to the software vendor. However, the software company can implement control activities to detect such reporting by comparing new software registration levels to sales volumes.

309 Further, risks pertaining to the complete and accurate recording of asset losses in the entity's financial statements represent a reporting objective. More specifically related to financial reporting, misstatements may arise from failing to record the loss of assets, manipulating the financial statements to conceal such a loss, or recording transactions outside the appropriate reporting period. For instance, an entity may hold its books open for an extended time after a period end to include additional sales, improperly account for intercompany transfers of inventory, or manipulate the amortization of its capital assets.

Safeguarding of Assets

310 Safeguarding of assets refers to protecting against the unauthorized and wilful acquisition, use, or disposal of assets. The inappropriate use of an entity's assets occurs to benefit an individual or group. The unauthorized acquisition, use, and disposal of assets may relate to activities such as illegal marketing, theft of assets, theft of intellectual property, late trading, and money laundering.

Relationship between Fraudulent Reporting and Safeguarding of Assets and Objectives

311 Safeguarding of assets typically relates to operations objectives, although certain aspects may relate to other categories of objectives. In terms of operations, management may consider the inappropriate use of an entity's assets and other resources including intellectual property and preventing loss through theft, waste, or neglect. An entity may also lose value of its assets through inefficiency or what turns out to be simply bad business decisions—such as selling a product at too low a price, or extending credit to bad risks. These situations relate to the operations objectives but are not directly linked to safeguarding of assets.

312 Where legal or regulatory requirements apply, management considers risks relating to safeguarding of assets in relation to compliance objectives. For example, an entity may intentionally prepare inaccurate regulatory reporting statements to avoid inspection and penalties.

313 Regardless of what objective may be affected, the responsibility and accountability for loss prevention and anti-fraud policies and procedures reside with management of the entity and its subunits in which the risk resides.

Corruption

314 In addition to assessing risks relating to the safeguarding of assets and fraudulent reporting, management considers possible corruption occurring within the entity. Corruption is generally relevant to the compliance category of objectives but could very well influence the control environment that also affects the entity's external financial reporting objectives. This includes considering incentives and pressures to achieve objectives while demonstrating adherence to expected standards of conduct and the effect of the control environment, specifically actions linked to Principle 4 (Demonstrates Commitment to Competence) and Principle 5 (Enforces Accountability). Aspects of corruption that are considered in an external financial reporting context typically relate to illegal acts that are considered in government statutes relevant to the activity.

315 In assessing possible corruption, the entity is not expected to directly manage the actions of personnel within third-party organizations, including those relating to outsourced operations, customers, suppliers, or advisors. However, depending on the level of risk assessed within this component, management may stipulate the expected level of performance and standards of conduct through contractual relations, and develop control activities that maintain oversight of third-party actions. Where necessary, management responds to detected unusual actions of others.

Management Override

316 Management override describes action taken to override an entity's controls for an illegitimate purpose including personal gain or an enhanced presentation of an entity's financial condition or compliance status. For example, to allow a large shipment of goods to a customer with unacceptable credit in order to increase revenue, a manager improperly overrides internal control by approving the sale transaction placed on credit hold by a supervisor who conducted the control properly. Actions to override are typically not documented or disclosed, because the intent is to cover up the actions.

317 Management override should not be confused with management intervention, which represents action that departs from controls designed for legitimate purposes. At times, management intervention is necessary to deal with non-recurring and non-standard transactions or events that otherwise might be handled inappropriately. Providing for management intervention is necessary because controls cannot be designed to anticipate and mitigate every risk and condition. Management's actions to intervene are generally overt and commonly documented or otherwise disclosed to appropriate personnel.

318 As part of assessing fraud risk, management assesses the risk of management override of internal control. The board of directors or subset of the board (e.g., audit committee) oversees this assessment and challenges management depending on the circumstances. This is especially important for smaller entities where senior management may be very involved in conducting many controls (e.g., in the period-end financial reporting process).

Factors Impacting Fraud Risk

Incentives and Pressures

319 Assessing the risk of fraud includes considering opportunities to commit fraud, as well as attitudes and rationalizations. Where there is a loss of assets, fraudulent reporting, or corruption, there are typically incentives and pressures, opportunities to access those assets, and attitudes and rationalizations that claim to justify the action. Incentives and pressures often result from and relate to the control environment, as discussed in Principle 5 (Enforces Accountability). As part of assessing fraud risk, the organization considers possible incentives and pressures and the potential impact on fraud risk.

Opportunity

320 Opportunity refers to the ability to actually acquire, use, or dispose of assets, which may be accompanied by altering the entity's records. Those involved in the inappropriate actions usually also believe that their activities will not be detected. Opportunity is created by weak control activities and monitoring, poor management oversight, and management override of control. For instance, the likelihood of a loss of assets or fraudulent external reporting increases when there is:

- A complex or unstable organizational structure
- High turnover rates of employees within accounting, operations, risk management, internal audit, or technology staff

- Ineffective design or poorly executed control activities
- Ineffective technology systems

Attitudes and Rationalization

321 Attitudes and rationalizations by individuals engaging in or justifying inappropriate actions may include:

- A person labeling the use of resources as borrowing, and fully intending to pay the stolen money back at some point
- A person believing that something is owed to him or her because of job dissatisfaction (salary, job environment, treatment by managers, etc.)
- A person not understanding or not caring about the consequences of his or her actions or of accepted notions of decency and trust

Other Considerations in Fraud Risk Assessment

322 It is possible to mitigate the likelihood of a fraud-related risk by taking action within the other components of internal control or by making changes to the entity's operating units, business processes, and activities. An entity may choose to sell certain operations that are prone to having higher risks relating to individual conduct, cease doing business in certain geographic locations, reallocate roles among personnel to enhance the segregation of duties, or reorganize its business processes to avoid unacceptable risks. For example, the risk of misappropriation of funds may be reduced by implementing a central payment processing function with greater segregation of duties instead of having only a few staff process payments at each of the entity's locations. The risk of corruption may be reduced by closely monitoring the entity's procurement process. The risk of financial statement fraud may be reduced by establishing shared services centers to provide accounting services to multiple segments, affiliates, or geographic locations of an entity's operations. A shared services center may be less vulnerable to influence by local operations managers and may be able to cost effectively implement more extensive anti-fraud programs.

323 When management detects fraudulent reporting, inadequate safeguarding of assets, or corruption, some form of remediation may be necessary. In addition to dealing directly with the improper actions, it may be necessary to take remediation steps within the risk assessment process or amend actions undertaken as part of other components of internal control.

Identifies and Analyzes Significant Change

Principle 9: The organization identifies and assesses changes that could significantly impact the system of internal control.

Points of Focus

324 The following points of focus may assist management in determining whether this principle is present and functioning:

- **Assesses Changes in the External Environment**—The risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates.
- **Assesses Changes in the Business Model**—The organization considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies.
- **Assesses Changes in Leadership**—The organization considers changes in management and respective attitudes and philosophies on the system of internal control.

Assessing Change

325 As economic, industry, and regulatory environments change, the scope and nature of an entity's leadership, priorities, business model, organization, business processes, and activities need to adapt and evolve. Internal control effective within one set of conditions may not necessarily be effective when those conditions change significantly. As part of risk assessment, management identifies changes that could significantly impact the entity's system of internal control and takes action as necessary. Thus, every entity will require a process to identify and assess those internal and external factors that can significantly affect its ability to achieve its objectives.

326 This process will parallel, or be a part of, the entity's regular risk assessment process. It involves identifying the changes to any significant assumption or condition. It requires having controls in place to identify and communicate changes that can affect the entity's objectives—and assess the associated risks. Such analysis includes identifying potential causes of achieving or failing to achieve an objective, assessing the likelihood that such causes will occur, evaluating the probable effect on achievement of the objectives, and considering the degree to which the risk can be managed.

327 Although the process by which an entity manages change is similar to, if not a part of, its regular risk assessment process, it is discussed separately. This is because it is

critically important to effective internal control and because it can too easily be overlooked or given insufficient attention in the course of dealing with everyday issues.

328 Management develops approaches to identify significant changes in any material assumption or condition that have taken place or will shortly occur. To the extent practicable, these mechanisms are forward looking, so an entity can anticipate and plan for significant changes. Early warning systems should be in place to identify information signaling new risks that can have a significant impact on the entity. Management also develops and implements controls relating to the conduct of such approaches.

329 This focus on change is founded on the premise that, because of their potential impact, certain conditions should be the subject of special consideration. The extent to which such conditions require management's attention, of course, depends on the effect they may have in particular circumstances.

The External Environment

- *Changing External Environment*—A changing regulatory or economic environment can result in increased competitive pressures, changes in operating requirements, and significantly different risks. Large-scale operations, reporting, and compliance failures by one entity may result in the rapid introduction of broad new regulations. For instance, the release of harmful materials near populated or environmentally sensitive areas may result in new industry-wide transportation restrictions that impact an entity's shipping logistics; the external information that is viewed as having poor transparency may result in enhanced regulatory reporting requirements for all publicly traded companies; and the poor treatment of elderly patients in a care facility may prompt additional care requirements for all care facilities. Each of these changes may require an organization to closely examine the design of its internal control system.
- *Changing Physical Environment*—Natural disasters directly impacting the entity, supply chain, and other business partners may result in elevated risks that an entity needs to consider to sustain its business. An organization, for example, may need to find alternative sources of raw material or move production.

Business Model

- *Changing Business Model*—When an entity enters new business lines, alters the delivery of its services through new outsourced relationships, or dramatically alters the composition of existing business lines, previously effective internal controls may no longer be relevant. The composition of the risks initially assessed as the basis for establishing internal controls may have changed, or the potential impact of those risks may have increased so that prior internal controls are no longer sufficient. Some financial services organizations, for example, may have expanded into new products and concentrations without focusing on how to respond to changes in the associated risks of their products.

- *Significant Acquisitions and Divestitures*—When an entity decides to acquire business operations, it may need to review and standardize internal controls across the expanded entity. Controls in place in the pre-acquisition operations may not be well developed, suitable for the newly combined entity, or scalable to operation in the new business. Similarly, when an operation is disposed of, the level of acceptable variation may change in operations, and materiality may decrease. In addition, certain entity-level controls at the disposed business operation may no longer be present. Both the acquisition and divesture of a business may require the organization to review and possibly revise its internal controls to support the achievement of objectives as appropriate to the restructured entity.
- *Foreign Operations*—The expansion or acquisition of foreign operations carries new and often unique risks. Developing business in new geographies or outsourcing operations to foreign locations may help the business to grow and/or reduce costs, but it may also present new challenges and alter the type and extent of the risks. Operating in unfamiliar markets poses risk because there are different customs and practices. For instance, the control environment in a new environment is likely to be influenced by the local culture and customs. Business risks may result from factors unique to the local economy and regulatory environment and channels of communication.
- *Rapid Growth*—When operations expand significantly and quickly, existing structures, business processes, information systems, or resources may be strained to the point where internal controls break down. For instance, adding manufacturing shifts to meet demand or increasing back-office personnel may result in those responsible for supervision being unable to adapt to the higher activity levels and maintain adequate control.
- *New Technology*—When new technologies are incorporated into production, service delivery processes, or supporting information systems, internal controls will likely need to be modified. For instance, introducing sales capabilities through mobile devices may require access controls specific to that technology as well as changes in controls over shipping processes.

Leadership Changes

- *Significant Personnel Changes*—A member of senior management new to an entity may not understand the entity's culture and reflect a different philosophy or may focus solely on performance to the exclusion of control-related activities. For instance, a newly hired chief executive officer focusing on revenue growth may send a message that a prior focus on effective internal control is now less important. Further, high turnover of personnel, in the absence of effective training and supervision, can result in breakdowns. For instance, a company that reduces its staffing levels by 25% in an attempt to reduce costs may erode the overall internal control structure.

7. Control Activities

Chapter Summary

330 Control activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews. Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, management selects and develops alternative control activities.

Principles relating to the Control Activities component

10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

11. The organization selects and develops general control activities over technology to support the achievement of objectives.

12. The organization deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Introduction

331 Control activities serve as mechanisms for managing the achievement of an entity's objectives and are very much a part of the processes by which an entity strives to achieve those objectives. They do not exist simply for their own sake or because having them is the right or proper thing to do.

332 Control activities can support one or more of the entity's operations, reporting, and compliance objectives. For example, an online retailer's controls over the security of its information technology affect the processing of accurate and valid transactions with consumers, the protection of consumers' confidential credit card information, and the availability and security of its website. In this case, control activities are necessary to support the reporting, compliance, and operations objectives.

Selects and Develops Control Activities

Principle 10: The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Points of Focus

333 The following points of focus may assist management in determining whether this principle is present and functioning:

- **Integrates with Risk Assessment**—Control activities help ensure that risk responses that address and mitigate risks are carried out.
- **Considers Entity-Specific Factors**—Management considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.
- **Determines Relevant Business Processes**—Management determines which relevant business processes require control activities.
- **Evaluates a Mix of Control Activity Types**—Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls.

- **Considers at What Level Activities Are Applied**—Management considers control activities at various levels in the entity.
- **Addresses Segregation of Duties**—Management segregates incompatible duties, and where such segregation is not practical management selects and develops alternative control activities.

Integration with Risk Assessment

334 Control activities support all the components of internal control, but are particularly aligned with the Risk Assessment component. Along with assessing risks, management identifies and puts into effect actions needed to carry out specific risk responses. Typically, control activities are not needed when an entity chooses to either accept or avoid a specific risk. There may, however, be instances where the organization decides to avoid a risk and chooses to develop control activities to avoid that risk. The action to reduce or share a risk serves as a focal point for selecting and developing control activities. The nature and extent of the risk response and any associated control activities will depend, at least in part, on the desired level of risk mitigation acceptable to management.

335 Control activities are those actions that help ensure that responses to assessed risks, as well as other management directives, such as establishing standards of conduct in the Control Environment, are carried out properly and in a timely manner. For example, a company sets an operations objective "to meet or exceed sales targets for the ensuing reporting period," and management identifies a risk that the organization's personnel have insufficient knowledge about current and potential customers' needs. Management's response to address this identified risk includes developing buying histories for existing customers and undertaking market research initiatives to increase the organization's understanding of how to attract potential customers. Control activities might include tracking the progress of the development of the customer buying histories against established timetables, and taking steps to help ensure the quality of the reported marketing data.

Relevant Business Processes

336 When determining what actions to put in place to mitigate risk, management considers all aspects of the entity's internal control components and the relevant business processes, information technology, and locations where control activities are needed. This may require considering control activities outside the operating unit, including shared service or data centers, and processes or functions performed in outsourced service providers. For example, entities may need to establish control activities to address the integrity of the information sent to and received from the outsourced service provider.

Entity-Specific Factors

337 Because each entity has its own set of objectives and implementation approaches, there will be differences in objectives, risk, risk responses, and related control activities. Even if two entities have identical objectives and structures, their control activities could

be different. Each entity is managed by different people with different skills who use individual judgment in effecting internal control. Moreover, controls reflect the environment and industry in which an entity operates, as well as the complexity of its organization, its history and its culture, nature, and scope of operations.

338 Entity-specific factors can impact the control activities needed to support the system of internal control. For instance:

- The environment and complexity of an entity, and the nature and scope of its operations, both physically and logically, affect its control activities.
- Highly regulated entities generally have more complex risk responses and control activities than less-regulated entities.
- The scope and nature of risk responses and control activities for multinational entities with diverse operations generally address a more complex internal control structure than those of a domestic entity with less-varied activities.
- An entity with a sophisticated enterprise resource planning system will have different control activities than an entity that uses an off-the-shelf computer accounting system.
- An entity with decentralized operations and an emphasis on local autonomy and innovation presents different control circumstances than another whose operations are constant and highly centralized.

Business Process Control Activities

339 Business processes are established across the entity to enable organizations to achieve their objectives. These business processes may be common to all businesses (such as purchasing, payables, or sales processing) or unique to a particular industry (such as claims processing, trust services, or drilling operations). Each of these processes transforms inputs into outputs through a series of transactions or activities.[11] Control activities that directly support the actions to mitigate transaction processing risks in an entity's business processes are often called "application controls" or "transaction controls."[12]

340 Transaction controls are the most fundamental control activities in an entity since they directly address risk responses in the business processes in place to meet management's objectives. Transaction controls are selected and developed wherever the business process may reside, ranging from the organization's financial consolidations process at the entity level to the customer support process at a particular operating unit.

341 A business process will likely cover many objectives and sub-objectives, each with its own set of risks and risk responses. A common way to consolidate these business

11 The term "transactions" tends to be associated with financial processes (e.g., payables transactions), while "activities" is more generally applied to operational or compliance processes. For the purposes of the Framework, the term "transactions" applies to both.

12 The term "transaction controls" is used in the Framework to refer to both manual and automated controls.

process risks into a more manageable form is to group them according to information-processing objectives[13] of completeness, accuracy, and validity.

342 If these information-processing objectives are achieved for each of the transactions within a particular business process, then the business process sub-objectives will likely be achieved.

343 The following information-processing objective definitions are used in the Framework:

- *Accuracy*—Transactions are recorded at the correct amount in the right account (and on a timely basis) at each stage of processing. For instance, transaction controls over data elements and master data, such as the item price in the vendor master file, can address the accuracy of processing a purchasing transaction. Accuracy in the context of an operational process can be defined to cover the broader concept of quality (e.g. the accuracy and precision of a manufactured part).
- *Completeness*—Transactions that occur are recorded. For instance, an organization can mitigate the risk of not processing all transactions with vendors by selecting actions and transaction controls that support that all invoice transactions are processed within the accounts payable business process.
- *Validity*—Recorded transactions represent economic events that actually occurred and were executed according to prescribed procedures. Validity is generally achieved through control activities that include the authorization of transactions as specified by an organization's established policies and procedures (i.e., approval by a person having the authority to do so). In an operational context, the parts used in making an automobile are obtained from an authorized supplier.

344 The risk of untimely transaction processing may be considered a separate risk or included as part of the completeness or accuracy information-processing objective. Restricted access is an important consideration for most business processes and is often included as an information-processing objective because without appropriately restricting access over transactions in a business process, the control activities in that business process can be overridden and segregation of duties may not be achieved.

345 Restricted access is especially important where technology is integral to an organization's processes or business. For example, many organizations use enterprise resource planning (ERP) applications. Configuring the security in these applications to address restricted access can become very complex and requires technical knowledge and a structured approach. Considerations for restricted access are discussed in more detail under the Security Management Processes section of Principle 11.

346 While the information-processing objectives are most often associated with financial processes and transactions, the concept can be applied to any activity in an organization. For instance, a candy maker will strive to have control activities in place to help

13 While related in concept and terminology, information-processing objectives and financial statement assertions are different. Financial statement assertions are specific to the reliability of financial reporting, while information-processing objectives apply to transaction processing.

ensure that all the ingredients are included in its cooking process (completeness), in the right amounts (accuracy), and from approved vendors whose products passed quality testing (validity).

347 As another example, the information-processing objectives and related control activities also apply to management's decision-making processes over critical judgments and estimates. In this situation, management should consider the completeness of the identification of significant factors affecting estimates for which it must develop and support assumptions. Similarly, management should consider the validity and reasonableness of those assumptions and the accuracy of its estimation models.

348 This does not mean that if management considers the information-processing objectives the organization will never make a faulty judgment or estimate; judgments and estimates are always subject to human error. However, when appropriate control activities are in place, and the information management uses is, in its judgment, accurate, complete, and valid, then the likelihood of better decision making is improved.

Types of Transaction Control Activities

349 A variety of transaction control activities can be selected and developed, including the following:

- *Authorizations and Approvals*—An authorization affirms that a transaction is valid (i.e., it represents an actual economic event). An authorization typically takes the form of an approval by a higher level of management or of verification and a determination if the transaction is valid. For example, a supervisor approves an expense report after reviewing whether the expenses seem reasonable and within policy. An example of an automated approval is where an invoice unit cost is automatically compared to the related purchase order unit cost within a pre-established tolerance level. Invoices within the tolerance level are automatically approved for payment. Those invoices outside the tolerance level are flagged for additional investigation.
- *Verifications*—Verifications compare two or more items with each other or compare an item with a policy, and perform a follow-up action when the two items do not match or the item is not consistent with policy. Examples include computer matching or a reasonableness check. Verifications generally address the completeness, accuracy, or validity of processing transactions.
- *Physical Controls*— Equipment, inventories, securities, cash, and other assets are secured physically (e.g., in locked or guarded storage areas with physical access restricted to authorized personnel) and are periodically counted and compared with amounts shown on control records.
- *Controls over Standing Data*—Standing data, such as the price master file, is often used to support the processing of transactions within a business process. Control activities over the processes to populate, update, and maintain the accuracy, completeness, and validity of this data are put in place by the organization.

- *Reconciliations*—Reconciliations compare two or more data elements and, if differences are identified, action is taken to bring the data into agreement. For example, a reconciliation is performed over daily cash flows with net positions reported centrally for overnight transfer and investment. Reconciliations generally address the completeness and/or accuracy of processing transactions.
- *Supervisory Controls*— Supervisory controls assess whether other transaction control activities (i.e., particular verifications, reconciliations, authorizations and approvals, controls over standing data, and physical control activities) are being performed completely, accurately, and according to policy and procedures. Management normally uses judgment to select and develop supervisory controls over higher risk transactions. For instance, a supervisor may review[14] whether an accounting clerk performs a reconciliation according to policy. This can be a high-level review (e.g., checking if the reconciliation spreadsheet has been completed) or a more detailed review, (e.g., checking to see if any reconciling items have been followed up and corrected or an appropriate explanation is provided).

350 Control activities can be preventive or detective, and organizations usually select a mix. The major difference is the timing of when the control activity occurs. A preventive control is designed to avoid an unintended event or result at the time of initial occurrence (e.g., upon initially recording a financial transaction or upon initiating a manufacturing process). A detective control is designed to discover an unintended event or result after the initial processing has occurred but before the ultimate objective has concluded (e.g., issuing financial reports or completing a manufacturing process). In both cases the critical part of the control activity is the action taken to correct or avoid an unintended event or result.

351 When selecting and developing control activities, the organization considers the precision of the control activity—that is, how exact it will be in preventing or detecting an unintended event or result. For example, suppose the purchasing manager of a company reviews all purchases over $1 million. This control activity may mitigate the risk of errors over $1 million, helping to cap the entity's exposure, but it does not cover all transactions. In contrast, an automated edit check that compares prices on all purchase orders to the price master file and produces a report of variances that is reviewed by a purchasing supervisor addresses accuracy for all transactions. Control activity precision is closely linked to the organization's risk tolerance for a particular objective (i.e., the tighter the risk tolerance, the more precise the actions to mitigate the risk and the related control activities need to be).

352 When selecting and developing control activities it is important to understand what a particular control is designed to accomplish (i.e., the specific risk response the control addresses) and whether it has been developed and implemented as designed to mitigate the risk . For example, in one entity sales orders undergo an automated or manual edit check that matches a customer's billing address and zip code to information in a standing data file of valid customer relationships. If the match fails, corrective action is taken. This control activity helps achieve the accuracy information-processing objective.

14 Supervisory reviews can be either control activities or monitoring activities. The difference is discussed further in Chapter 9, Monitoring Activities.

353 However, it does not help achieve the completeness information-processing objective (i.e., whether all approved sales orders are being processed). Another control activity, such as sequentially numbering approved sales orders and then checking if all have been processed, would be needed to address completeness.

Technology and Control Activities

354 Control activities and technology[15] relate to each other in two ways:

- *Technology Supports Business Processes*—When technology is embedded into the entity's business processes, such as robotic automation in a manufacturing plant, control activities are needed to mitigate the risk that the technology itself will not continue to operate properly to support the achievement of the organization's objectives.
- *Technology Used to Automate Control Activities*—Many control activities in an entity are partially or wholly automated using technology. These procedures are known as automated control activities or automated controls in the Framework. Automated controls include financial process–related automated transaction controls, such as a three-way match performed within an ERP system supporting the procurement and payables sub-processes, and computerized controls in operational or compliance processes, such as checking the proper functioning of a power plant. Sometimes the control activity is purely automated, such as when a system detects an error in the transmission of data, rejects the transmission, and automatically requests a new transmission. Other times there is a combination of automated and manual procedures. For example, the system automatically detects the error in transmission, but someone has to manually force the re-transmission. In other cases, a manual control depends on information from a system, such as computer-generated reports supporting a budget-to-actual analysis.

355 Most business processes have a mix of manual and automated controls, depending on the availability of technology in the entity. Automated controls tend to be more reliable, subject to whether technology general controls, discussed later in this chapter, are implemented and operating, since they are less susceptible to human judgment and error, and are typically more efficient.

356 Those control activities over technology that are designed to support the continued operation of technology and automated control activities are known as "technology general controls" and are covered in Principle 11.

Control Activities at Different Levels

357 In addition to controls that operate at the transaction-processing level, the organization selects and develops a mix of control activities that operate more broadly and that typically take place at higher levels in the organization. These broader control activities

15 "Technology" is a broad term. In the Framework its use applies to technology that is computerized, including software applications running on a computer, manufacturing controls systems, etc.

usually are business performance or analytical reviews[16] involving comparisons of different sets of operating or financial data. The relationships are analyzed and investigated and corrective actions are taken when not in line with policy or expectations. Transaction controls and business performance reviews at different levels work together to provide a layered approach to addressing the organization's risks and are integral to the mix of controls within the organization.

358 For example, an operating unit may have business performance reviews over the procurement process that include purchase price variances, the percentage of orders that are rush purchase orders, and the percentage of returns to total purchase orders. By investigating any unexpected results or unusual trends, management may detect circumstances where the underlying procurement objectives may not have been achieved.

359 Another form of business performance review occurs when senior management conducts reviews of actual performance versus budgets, forecasts, prior periods, and competitor results. Major initiatives are tracked—such as marketing programs, improvements to production processes, and cost containment or reduction programs—to measure the extent to which targets are being reached. Management reviews the status of new product development, joint venture opportunities, or financing needs. Management actions taken to analyze and follow up on such reporting are control activities.

360 The scope of a business performance review (i.e., how many detailed risks it covers) will tend to be greater than for a transaction control. Also, the span of the review across the organization will tend to be greater as they are usually performed at higher levels in the organization than a transaction control. However, to effectively respond to a set of risks, the review must be precise enough to detect all errors that exceed the risk tolerance. A transaction control may address a single specific risk, whereas an operating unit business performance review typically addresses a number of risks. For example, the business performance review over rush purchase orders covers several risks in the procurement process but may not address risks concerning the accuracy and completeness of processing specific transactions.

361 Most business performance reviews are detective in nature because they typically occur after transactions have already taken place and been processed. So while higher-level controls are important in the mix of control activities, it is difficult to fully and efficiently address business process risks without transaction controls.

Segregating Duties

362 When selecting and developing control activities management should consider whether duties are divided or segregated among different people to reduce the risk of error or inappropriate or fraudulent actions. Such consideration should include the legal

16 Business performance reviews can be either control activities or monitoring activities. The difference is discussed further in Chapter 9, Monitoring Activities.

environment, regulatory requirements, and stakeholder expectations. This segregation of duties generally entails dividing the responsibility for recording, authorizing, and approving transactions, and handling the related asset. For instance, a manager authorizing credit sales is not responsible for maintaining accounts receivable records or handling cash receipts. If one person is able to perform all these activities he or she could, for example, create a fictitious sale that could go undetected. Similarly, salespersons should not have the ability to modify product price files or commission rates. A control activity in this area could include reviewing access requests to the system to determine whether segregation of duties is being maintained. For example, a request for the salesperson to have system access to modify product price files or commission rates should be rejected.

363 The segregation of duties can address important risks relating to management override. Management override circumvents existing controls and is an often-used means of committing fraud. The segregation of duties is fundamental to mitigating fraud risks because it reduces, but can't absolutely prevent, the possibility of one person acting alone. However, there is always the risk that management can override control activities. Collusion is needed to perform fraudulent activities when key process responsibilities are divided between at least two employees. Also, the segregation of duties reduces errors by having more than one person performing or reviewing transactions in a process, increasing the likelihood of an error being found.

364 However, sometimes segregation is not practical, cost effective, or feasible. For instance, small companies may lack sufficient resources to achieve ideal segregation, and the cost of hiring additional staff may be prohibitive. In these situations, management institutes alternative[17] control activities. In the example above, if the salesperson can modify product price files, a detective control activity can be put in place to have personnel unrelated to the sales function periodically review whether and under what circumstances the salesperson changed prices.

17 The Framework prefers the term "alternative controls" over "compensating controls." The latter term has been used to describe additional control activities put in place when segregation of duties could not be achieved. However, this term has evolved to refer to control activities that mitigate the impact of an identified control deficiency when evaluating the operating effectiveness of controls and is used in this context in the Framework.

Selects and Develops General Controls over Technology

Principle 11: The organization selects and develops general control activities over technology to support the achievement of objectives.

Points of Focus

365 The following points of focus may assist management in determining whether this principle is present and functioning:

- **Determines Dependency between the Use of Technology in Business Processes and Technology General Controls**—Management understands and determines the dependency and linkage between business processes, automated control activities, and technology general controls.
- **Establishes Relevant Technology Infrastructure Control Activities**—Management selects and develops control activities over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.
- **Establishes Relevant Security Management Process Control Activities**—Management selects and develops control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats.
- **Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities**—Management selects and develops control activities over the acquisition, development, and maintenance of technology and its infrastructure to achieve management's objectives.

Dependency between the Use of Technology in Business Processes and Technology General Controls

366 The reliability of technology within business processes, including automated controls, depends on the presence and proper functioning of the general control activities over technology, referred to from here on as technology general controls.[18] For instance, an automated matching and edit check examines data entered on-line. If something does not match, or is in the wrong format, immediate feedback is provided so that corrections can be made. Error messages indicate what is wrong with the data, and exception reports allow for subsequent follow-up.

367 Technology general controls must be deployed for automated controls to work properly when first developed and implemented (e.g., the automated control mentioned above edit checks match data with the right transaction or standing data file, any error message completely and accurately reflects what is wrong, and all exceptions are reported according to the entity's policies). Technology general controls also help information systems continue to function properly after they are implemented. The automated matching transaction control will work properly only if technology general controls are designed, implemented, and operating so that the right files are being used in the matching process and the files are complete and accurate. Also, proper security limits access to the system to only those who need it, reducing the possibility of unauthorized edits to the files. Control activities over any changes to the technology help ensure that it continues to function as designed.

368 As with other entity functions, processes are put in place to select, develop, operate, and maintain an entity's technology. These processes may be limited to a few activities over the use of standard technology purchased from an external party (e.g., a spreadsheet application) or expanded to support both in-house and externally developed technology. Selected and developed control activities contribute to the mitigation of specific risks surrounding the use of technology processes.

Technology General Controls

369 Technology general controls include control activities over the technology infrastructure, security management, and technology acquisition, development, and maintenance. They apply to all technology—from information technology applications on a mainframe computer, to client/server, desktop, end-user computing, portable computer, and mobile device environments, to operational technology, such as plant control systems or manufacturing robotics. The extent and rigor of control activities will vary for each of these technologies depending on various factors, such as the complexity of the technology and risk of the underlying business process being supported. Similar to business transaction controls, technology general controls may include both manual and automated control activities.

18 Terminology typically used to describe these controls includes "general computer controls," "general controls," or "information technology controls." The term "technology general controls" is used here to refer to "general control activities over technology."

Technology Infrastructure

370 Technology requires an infrastructure in which to operate, ranging from communication networks for linking technologies to each other and the rest of the entity, to the computing resources for applications to operate, to the electricity to power the technology. The technology infrastructure can be complex. It may be shared by different business units within the entity (e.g., a shared service center) or outsourced either to third-party service organizations or to location-independent technology services (e.g., cloud computing). These complexities present risks that need to be understood and addressed. Given the broad range of possible changes in the use of technology likely to continue into the future, the organization needs to track these changes and assess and respond to the new risks.

371 Control activities support the completeness, accuracy, and availability of technology processing. Whether the infrastructure is batch scheduling for a mainframe computer, real-time processing in a client/server environment, mobile wireless devices, or a sophisticated communications network, the technology is actively checked for problems and corrective action taken when needed. Maintaining technology often includes backup and recovery procedures, as well as disaster recovery plans, depending on the risks and consequences of a full or partial outage.

Security Management Processes

372 Security management includes sub-processes and control activities over who and what has access to an entity's technology, including who has the ability to execute transactions. They generally cover access rights at the data, operating system (system software), network, application, and physical layers. Security controls over access protects an entity from inappropriate access and unauthorized use of the system and supports segregation of duties. By preventing unauthorized use of and changes to the system, data and program integrity are protected from malicious intent (e.g., someone breaking into the technology to commit fraud, vandalism, or terrorism) or a simple error (e.g., a well-intentioned employee using a vacationing colleague's account to get work done, and executing a transaction erroneously or deleting a file because he or she is not properly trained in the work).

373 Security threats can come from both internal and external sources. The external threat is particularly important for entities that depend on telecommunications networks and the Internet. Technology users, customers, and malicious parties may be halfway around the world or down the hall. The many potential uses of technology and points of entry underscore the importance of security management. External threats have become prevalent in today's highly interconnected business environments, and continual effort is required to address these risks.

374 Internal threats may come from former or disgruntled employees who pose unique risks because they may be both motivated to work against the entity and better equipped to succeed in carrying out a malicious act because they have greater access and knowledge of the entity's security management systems and processes.

375 User access to technology is generally controlled through authentication control activities where a unique user identification or token is authenticated against an approved list. Technology general controls are designed to allow only authorized users on an

approved list. These control activities generally employ a policy of restricting authorized users to the applications or functions commensurate with their job responsibilities and supporting an appropriate segregation of duties. Control activities are used to check requests for access against the approved list. Other control activities are in place to update access when employees change job functions or leave the entity. A periodic review of access rights against the policy is often used to check if access remains appropriate. Access also needs to be controlled when different technology elements are connected to each other.

Technology Acquisition, Development, and Maintenance Processes

376 Technology general controls support the acquisition, development, and maintenance of technology. For example, a technology development methodology[19] provides a structure for system design and implementation, outlining specific phases, documentation requirements, approvals, and checkpoints with controls over the acquisition, development, and maintenance of technology. The methodology provides appropriate controls over changes to technology, which may involve requiring authorization of change requests, reviewing the changes, approvals, and testing results, and implementing protocols to determine whether changes are made properly.

377 In some companies the development methodology covers the continuum from large development projects to the smallest changes. In other companies there is one distinct process for developing new technology and a separate process for change management. In either case, a change management process will be in place to track changes from initiation to final disposition. Changes may arise as a result of a problem in the technology that needs to be fixed or a request from the user community.

378 The technology general controls included in a development methodology will vary depending on the risks of the technology initiative. A large or complex development initiative will generally have greater risks than a small or simple initiative. The extent and rigor of the controls over the initiative should be sized accordingly.

379 One alternative to in-house development is the use of packaged software. Technology vendors provide flexible, integrated systems allowing customization through the use of built-in options. Many technology development methodologies address the acquisition of vendor packages as a development alternative and include the necessary steps to provide control over their selection and implementation. Once selected and implemented, technology general controls outlined above would also apply to the ongoing development and maintenance of technology,

380 Another alternative is outsourcing. While in principle the same considerations apply whether controls are performed internally or by an outsourced service provider, outsourcing presents unique risks and often requires selecting and developing additional controls over the completeness, accuracy, and validity of information submitted to and received from the outsourced service provider.

19 There are many names for this process. One common name is "systems development life cycle" (SDLC).

Deploys through Policies and Procedures

Principle 12: The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Points of Focus

381 The following points of focus may assist management in determining whether this principle is present and functioning:

- **Establishes Policies and Procedures to Support Deployment of Management's Directives**—Management establishes control activities that are built into business processes and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions.
- **Establishes Responsibility and Accountability for Executing Policies and Procedures**—Management establishes responsibility and accountability for control activities with management (or other designated personnel) of the business unit or function in which the relevant risks reside.
- **Performs in a Timely Manner**—Responsible personnel perform control activities in a timely manner as defined by the policies and procedures.
- **Takes Corrective Action**—Responsible personnel investigate and act on matters identified as a result of executing control activities.
- **Performs Using Competent Personnel**—Competent personnel with sufficient authority perform control activities with diligence and continuing focus.
- **Reassesses Policies and Procedures**—Management periodically reviews control activities to determine their continued relevance, and refreshes them when necessary.

Policies and Procedures

382 Policies reflect management's statement of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through management's actions and decisions. Procedures consist of actions that implement a policy.

383 Control activities specifically relate to those policies and procedures that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. A policy, for instance, might call for review of customer trading activities by a securities dealer retail branch manager. The procedure is the review itself, performed in a timely manner and with attention given to factors set forth in the policy, such as the nature and volume of securities traded, and their relation to customer net worth and age.

384 Policies and procedures are often communicated orally. Unwritten policies can be effective where the policy is a long-standing and well-understood practice, and in smaller organizations where communications channels involve limited management layers and close interaction with and supervision of personnel. Though a cost-effective alternative for some entities, unwritten policies and procedures can be easier to circumvent, costly to the organization if there is turnover in personnel, and reduce accountability. When subject to external party review, policies and procedures would be expected to be formally documented.[20]

385 But whether or not a policy is in writing, it must establish clear responsibility and accountability, which ultimately resides with the management of the entity and subunit where the risk resides. Procedures should be clear on the responsibilities of personnel performing the control activity. Also, policies need to be deployed thoughtfully and conscientiously, and the related procedures must be timely and be performed diligently and consistently by competent personnel.

Timeliness

386 The procedures should include the timing of when a control activity and any follow-up corrective actions are performed. Untimely procedures can reduce the usefulness of the control activity. For example, a regular review of user accounts for inappropriate access rights is conducted by the business process owner on a timely basis to reduce the risk of unauthorized access to an acceptable level. Longer intervals between reviews increase the potential for untimely detection of unauthorized access.

Corrective Action

387 In conducting a control activity, matters identified for follow-up should be investigated and, if appropriate, corrective action taken. For example, consider a case where a reconciliation of cash accounts detects a discrepancy in one of the accounts. The accounting clerk follows up with the person in charge of recording cash and determines that a cash receipt was not posted properly. The receipt is reapplied and the correction is reflected in the reconciliation.

20 See the discussion on documentation in Chapter 4, Additional Framework Considerations.

Competence

388 A well-designed control activity generally cannot be conducted without competent personnel. The level of competency required to perform a control activity will depend on factors such as the complexity of the control activity and the complexity and volume of the underlying transactions. Furthermore, a procedure will not be useful if performed by rote, without a sharp, continuing focus on the risks to which the policy is directed.

Periodic Reassessment

389 Management should periodically reassess policies and procedures and related control activities for continued relevance and effectiveness, unrelated to being responsive to significant changes in the entity's risks or objectives. Significant changes would be evaluated through the risk assessment process. Changes in people, process, and technology may reduce the effectiveness of control activities or make some control activities redundant. Whenever one of these changes occurs, management should reassess the relevance of the existing controls and refresh them when necessary. For example, management may upgrade the purchasing module of an ERP system and introduce automated transaction control activities that cause the old manual control activities to be redundant and, hence, no longer necessary.

8. Information and Communication

Chapter Summary

390 Information is necessary for the entity to carry out internal control responsibilities to support the achievement of its objectives. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of other components of internal control. Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is the means by which information is disseminated throughout the organization, flowing up, down, and across the entity. It enables personnel to receive a clear message from senior management that control responsibilities must be taken seriously. External communication is twofold: it enables inbound communication of relevant external information and provides information to external parties in response to requirements and expectations.

Principles relating to the Information and Communication component

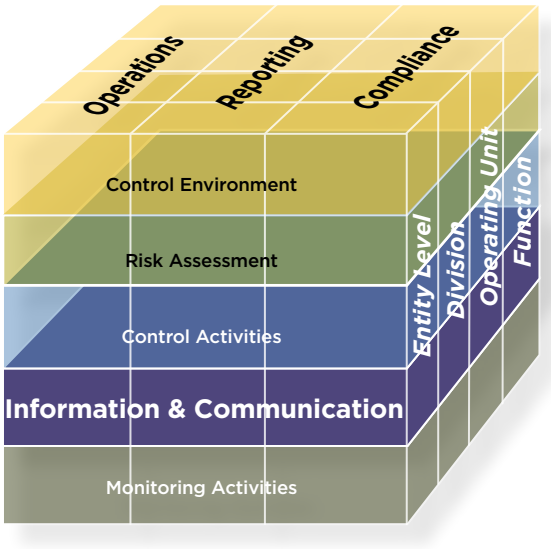
13. The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.

14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of other components of internal control.

15. The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.

Introduction

391 The Information and Communication component of the Framework supports the functioning of all components of internal control. In combination with the other components, information and communication supports the achievement of the entity's objectives, including objectives relevant to internal and external reporting. Controls within Information and Communication support the organization's ability to use the right information within the system of internal control and to carry out internal control responsibilities.



392 Information is the data that is combined and summarized based on relevance to information requirements. Information requirements are determined by the ongoing functioning of the other internal control components, taking into consideration the expectations of all users, both internal and external. Information systems support informed decision making and the functioning of the other components of internal control by processing relevant, timely, and quality information from internal and external sources.

393 Communication enables the organization to share relevant and quality information internally and externally. Management communicates information internally to enable personnel to understand the entity's objectives and the importance of their control responsibilities. Internal communication facilitates the functioning of other components of internal control by sharing information up, down, and across the entity. External communication enables management to obtain and share information between the entity and external parties about risks, regulatory matters, changes in circumstances, customer satisfaction, and other information relevant to the functioning of the other components of internal control.

394 An information system is the set of activities, involving people, processes, data and/or technology, which enable the organization to obtain, generate, use, and communicate transactions and information to maintain accountability and measure and review the entity's performance or progress toward achievement of objectives.

395 The Framework distinguishes this component from the internal reporting category of objectives. Information and Communication is only one component of the Framework. Controls within this component help to provide relevant, quality information to support all components of internal control. On the other hand, an organization seeking reasonable assurance regarding a specified reporting objective is achieved through all five components of internal control being present and functioning, and operating together.

396 Communication relates to sharing information used in designing, implementing, or conducting internal control, or in assessing its effectiveness. Communication can appear broad at times (e.g., information communicated about external trends or events), but when it is used in the context of the Framework, this communication may enable a user to carry out controls within Risk Assessment.

Uses Relevant Information

Principle 13: The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.

Points of Focus

397 The following points of focus may assist management in determining whether this principle is present and functioning:

- **Identifies Information Requirements**—A process is in place to identify the information required and expected to support the functioning of the other components of internal control and the achievement of the entity's objectives.
- **Captures Internal and External Sources of Data**—Information systems capture internal and external sources of data.
- **Processes Relevant Data into Information**—Information systems process and transform relevant data into information.
- **Maintains Quality throughout Processing**—Information systems produce information that is timely, current, accurate, complete, accessible, protected, and verifiable and retained. Information is reviewed to assess its relevance in supporting the internal control components.
- **Considers Costs and Benefits**—The nature, quantity, and precision of information communicated are commensurate with and support the achievement of objectives.

Information Requirements

398 Information is necessary for the organization to carry out its internal control responsibilities to support the achievement of objectives. Information about the entity's objectives is gathered from board and senior management activities and summarized in a way that management and others can understand objectives and their role in their achievement.

399 For example, a wholesale distributor found that its managers did not have a solid understanding of the key objectives for the organization. The business plan was detailed and difficult to concisely communicate. The board of directors worked with senior management to summarize the entity's key objectives into a clear narrative document that accompanied internally distributed financial statements. In addition, they provided a balanced scorecard that mapped these goals to metrics and actual results, both non-financial and financial, on a monthly basis. Feedback from a subsequent employee survey indicated that management and other personnel better understood the organization's objectives.

400 Obtaining relevant information requires management to identify and define information requirements at the relevant level and requisite specificity. Identifying information requirements is an iterative and ongoing process that occurs throughout the performance of an effective internal control system.

401 Management develops and implements controls relating to the identification of relevant information that support the functioning of other components. The following examples illustrate how information in support of the functioning of other internal control components is identified and defined.

Internal Control Component	Example of Information Used
Control Environment	Management performs an annual entity-wide survey of its employees to gather information about their personal conduct in relation to the entity's code of conduct. The survey is part of a process that produces information to support the control environment component and may also provide input into the selection, development, implementation, or maintenance of control activities.
Risk Assessment	As a result of changes in customer demands, an entity changes its product mix and delivery mechanisms. Expanded on-line sales have caused credit card transactions to increase significantly. To assess the risk of non-compliance with security and privacy regulations associated with credit card information, management gathers information about the number of transactions, overall value, and nature of data retained for the last fiscal year and evaluates its significance in conducting its risk analysis.
Control Activities	Certain equipment used in a high-volume production environment deteriorates if it operates longer than a specified time period. To maximize equipment lifespan, management obtains and reviews the daily up-time logs and compares them to ranges set by senior management. The information supports control activities that address mitigation procedures required when maximum up-time levels are exceeded.
Monitoring Activities	A large utility company gathers, processes, and reports accident and injury records related to the power generation operating unit. Comparing this information with trends in workers' compensation health insurance claims identifies variations from established expectations. This may indicate that control activities over the identification, processing, reporting, investigation, and resolution of accident and injury events may not be functioning as intended.

402 Information requirements are established through activities performed in support of the other internal control components. These requirements facilitate and direct management and other personnel to identify relevant and reliable sources of information and underlying data. The amount of information and underlying data available to management may be more than is needed because of increased sources of information and

advances in data collection, processing, and storage. In other cases, data may be difficult to obtain at the relevant level or requisite specificity. Therefore, a clear understanding of the information requirements directs management and other personnel to identify relevant and reliable sources of information and data.

403 Achieving the right balance between the benefits and the costs to obtain and manage information, and the information systems, is a key consideration in establishing an information system that meets the entity's needs.

Information from Relevant Sources

404 Information is received from a variety of sources and in a variety of forms. The following table summarizes examples of internal and external data and sources from which management can generate useful information relevant to internal controls.

Examples of Internal Sources of Data	Examples of Internal Data
• Email communications	• Organizational changes
• Inspections of production floor processing	• On-time and quality production experience
• Minutes or notes from operating committee meetings	• Actions in response to energy consumption metrics
• Personnel time reporting system	• Hours incurred on time-based projects
• Reports from manufacturing systems	• Number of units shipped in a month
• Responses to customer surveys	• Factors impacting customer attrition rates
• Whistle-blower hotline	• Complaint on manager's behavior

Examples of External Sources of Data	Examples of External Data
Data received from outsourced service providers	Products shipped from contract manufacturer
Industry research reports	Competitor product information
Peer company earnings releases	Market and industry metrics
Regulatory bodies	New or expanded requirements
Social media or other blog posts	Opinions about the entity
Trade shows	Evolving customer preferences
Whistle-blower hotline	Claim of misuse of funds, bribery

405 Management considers a comprehensive scope of potential events, activities, and data sources, available internally and from reliable external sources, and selects the most relevant and useful to the current organizational structure, business model, or objectives. As change in the entity occurs, the information requirements also change. For example, entities operating in a highly dynamic business and economic environment experience continual changes such as highly innovative and quick-moving competitors, shifting customer expectations, evolving regulatory requirements, globalization, and technology innovation. Therefore, management re-evaluates information requirements and adjusts to meet its ongoing needs.

Processing Data through Information Systems

406 Organizations develop information systems to source, capture, and process large volumes of data from internal and external sources into meaningful, actionable information to meet defined information requirements. Information systems encompass a combination of people, processes, data, and technology that support business processes managed internally as well as those that are supported through relationships with outsourced service providers and other parties interacting with the entity.

407 Information may be obtained through a variety of forms including manual input or compilation, or through the use of information technology such as electronic data interchange (EDI) or application programming interfaces (API). Conversations with customers, suppliers, regulators, and employees are also sources of critical data and information needed to identify and assess both risks and opportunities. In some instances, information and underlying data captured requires a series of manual and automated processes to ensure it is at the relevant level and requisite specificity. In other cases, information may be obtained directly from an internal or external source. Management develops and implements controls over the integrity of data input into information systems and over the completeness and accuracy of processing such data into information used by other controls.

408 The volume of information accessible to the organization presents both opportunities and risks. Greater access to information can enhance internal control. On the other hand, increased volume of information and underlying data may create additional risks such as operational risks caused by inefficiency due to data overload; compliance risks associated with laws and regulations around data protection, retention; and privacy and security risks arising from the nature of data stored by or on behalf of the entity.

409 The nature and extent of information requirements, the complexity and volume of information, and the dependence on external parties impacts the range of sophistication of information systems, including the extent of technology deployed. Regardless of the level of sophistication adopted, information systems represent the end-to-end information processing of transactions and data that enable the entity to collect, store, and summarize quality and consistent information across the relevant processes, whether manual, automated, or a combination of both.

410 Information systems developed with integrated, technology-enabled processes provide opportunities to enhance the efficiency, speed, and accessibility of information to users. Additionally, such information systems may enhance internal control over security and privacy risks associated with information obtained and generated by the organization. Information systems designed and implemented to restrict access to information only to those who need it and to reduce the number of access points enhance the effectiveness of mitigating risks associated with the security and privacy of information.

411 Enterprise resource planning (ERP) systems, association management systems (AMS), corporate intranets, collaboration tools, interactive social media, data warehouses, business intelligence systems, operational systems (e.g., factory automation and energy-usage systems), web-based applications, and other technology solutions present opportunities for management to leverage technology in developing and implementing effective and efficient information systems.

Information Quality

412 Maintaining quality of information is necessary to an effective internal control system, particularly with today's volume of data and dependence on sophisticated, automated information systems. The ability to generate quality information begins with the quality of data sourced. Inaccurate or incomplete data, and the information derived from such data, could result in potentially erroneous judgments, estimates, or other management decisions.

413 The quality of information depends on whether it is:

- *Accessible*—The information is easy to obtain by those who need it. Users know what information is available and where in the information system the information is accessible.
- *Correct*—The underlying data is accurate and complete. Information systems include validation checks that address accuracy and completeness, including necessary exception resolution procedures.
- *Current*—The data gathered is from current sources and is gathered at the frequency needed.
- *Protected*—Access to sensitive information is restricted to authorized personnel. Data categorization (e.g., confidential and top secret) supports information protection.
- *Retained*—Information is available over an extended period of time to support inquiries and inspections by external parties.
- *Sufficient*—There is enough information at the right level of detail relevant to information requirements. Extraneous data is eliminated to avoid inefficiency, misuse, or misinterpretation.
- *Timely*—The information is available from the information system when needed. Timely information helps with the early identification of events, trends, and issues.
- *Valid*—Information is obtained from authorized sources, gathered according to prescribed procedures, and represents events that actually occurred.
- *Verifiable*—Information is supported by evidence from the source. Management establishes information management policies with clear responsibility and accountability for the quality of the information.

414 These policies also address data governance expectations that guide processes to define categories or classes of data and assign requirements for physical handling, storage, security, and privacy. These policies support management and other personnel's responsibilities for protecting data and information from unauthorized access or change and for adhering to retention requirements.

415 For example, in one case senior management of a decentralized, geographically dispersed government agency identified a risk, specific to achieving an operational objective, associated with the quality of operational data collected from its 2,000 field units. Management developed a set of specified data requirements and a reporting format to be used by all field units. Senior management consistently performed monthly reviews of key metrics derived from the data across all units. Those units with the best and poorest performance were required to explain the source of their data to an internal audit team. In addition, agency management used the reports of unit operational data and metrics on field visits and began asking questions to assess the unit's understanding of data on the reports. After six months of implementing this system of reporting, monthly reviews and field visits, and the related feedback that was shared throughout the process, the quality of information improved to the level acceptable to management. To maintain this level, management implemented amended policies and processes for reporting the operational data and business intelligence technology to enable consistent, timely reporting of the information.

416 Information that is obtained from outsourced service providers that manage business processes on behalf of the entity, and other external parties on whom the entity depends, is subject to the same internal control expectations. Information requirements are developed by the organization and communicated to outside service providers and other similar external parties. Controls support the organization's ability to rely on such information, including internal control over outsourced service providers such as vendor due diligence, exercise of right-to-audit clauses, and obtaining an independent assessment over the service provider's controls.

417 Management considers its requirements to retain communications, particularly those to and from external parties or those that relate to the entity's compliance with laws and regulations. Given the potential volume and ability to store and retrieve such information, this requirement may be challenging when management relies on real-time, technology-enabled communication. Controls over retention of internal control information consider the challenges of advances in technology, including communication and collaboration technologies used to support other components of internal control and achievement of the entity's objectives.

Communicates Internally

Principle 14: The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of other components of internal control.

Points of Focus

418 The following points of focus may assist management in determining whether this principle is present and functioning:

- **Communicates Internal Control Information**—A process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities.
- **Communicates with the Board of Directors**—Communication exists between management and the board of directors so that both have information needed to fulfill their roles with respect to the entity's objectives.
- **Provides Separate Communication Lines**—Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.
- **Selects Relevant Method of Communication**—The method of communication considers the timing, audience, and nature of the information.

Internal Control Communication

419 Communication of information conveyed across the entity include:

- Policies and procedures that support personnel in performing their internal control responsibilities
- Specified objectives
- Importance, relevance, and benefits of effective internal control
- Roles and responsibilities of management and other personnel in performing controls
- Expectations of the organization to communicate up, down, and across the entity any matters of significance relating to internal control including instances of weakness, deterioration, or non-adherence

420 The organization establishes and implements policies and procedures that facilitate effective internal communication. This includes specific and directed communication that addresses individual authorities, responsibilities, and standards of conduct across

the entity. Senior management communicates the entity's objectives clearly through the organization so that other management and personnel, including non-employees such as contractors, understand their individual roles in the organization. Such communication occurs regardless of where personnel are located, their level of authority, or their functional responsibility. Internal communication begins with the communication of specified objectives. As management cascades the communication of the entity-specific objectives throughout the organization, it is important that the related sub-objectives or specific requirements are communicated to personnel in a manner that allows them to understand how their roles and responsibilities impact the achievement of the entity's objectives.

421 All personnel also receive a clear message from senior management that their internal control responsibilities must be taken seriously. Through communication of objectives and sub-objectives, personnel understand how their roles, responsibilities, and actions relate to the work of others in the organization, their responsibilities for internal control, and what is deemed acceptable and unacceptable behavior. As discussed under Control Environment, by establishing appropriate structures, authorities, and responsibilities, communication to personnel of the expectations for internal control is effected. However, communication about internal control responsibilities may not on its own be sufficient to ensure that management and other personnel embrace their accountability and respond as intended. Often, management must take timely action that is consistent with such communication to reinforce the messages conveyed.

422 Management selects, develops and deploys controls over the sharing of information through internal communication and that help management and other personnel leverage information that may impact multiple functions, operating units or divisions. For example:

- Field service personnel in the sales department of an entity gather information about defect rates on certain parts. This information is also useful to the directors of manufacturing and engineering as it may indicate a production quality or product design issue. In addition, the results of monitoring activities are communicated to other personnel to help identify the root cause of an issue and take corrective action.
- Internal audit department conducts an audit over the commissions paid to distributors in one international location. The audit reveals instances of fraudulent reporting of sales through certain distributors. Further investigation exposes payments by the distributor to the sales representative responsible for the related distributors. In addition to sharing information with those responsible for responding to potential fraud, it is shared with sales management in other international locations, enabling them to analyze information more critically to determine if the issue is more pervasive and take any necessary actions.

Internal Control Communication with Board

423 Communication between management and the board of directors provides the board with information needed to exercise its oversight responsibility for internal control. Information relating to internal control communicated to the board generally includes significant matters about the adherence to, changes in, or issues arising from the system of internal control. The frequency and level of detail of communication between management and the board of directors must be sufficient to enable the board of directors to understand the results of management's separate and ongoing assessments and the impact of those results on the achievement of objectives. Additionally, the frequency and level of detail must be sufficient to enable the board of directors to respond to indications of ineffective internal control in a timely basis.

424 Direct communication to the board of directors by other personnel is also important. Members of the board of directors should have direct access to employees without interference from management. For example, some organizations encourage board members to meet with management and personnel without senior management present. This allows board members to independently ask questions and assess important matters that employees may not otherwise feel comfortable sharing, such as adherence to the code of conduct, competence of personnel, or potential management override of controls. Additionally, the overall system of internal control is enhanced by the internal audit department that is independent of management. Internal audit communication to the board of directors is generally direct, free from management bias and, where necessary, confidential.

Communication beyond Normal Channels

425 For information to flow up, down, and across the organization, there must be open channels of communication and a clear-cut willingness to report and listen. Management and other personnel must believe their supervisors truly want to know about problems and will deal with them, as necessary. In most cases, normal established reporting lines in an entity are the appropriate channels of communication. However, personnel are quick to pick up on signals if management does not have the time, interest, or resources to deal with problems they have uncovered. Compounding the problem is that an unreceptive or unavailable manager is usually the last to know that the normal communications channel is inoperative or ineffective.

426 In some circumstances, separate lines of communication are needed to establish a fail-safe mechanism for anonymous or confidential communication when normal channels are inoperative or ineffective. Many entities provide, and make employees aware of, a channel for such communications to be received by the board of directors or a board delegate such as a member of the audit committee. In some cases, laws and regulations require companies to establish such alternative communications channels (e.g., whistle-blower and ethics hotlines). Information systems should include mechanisms for anonymous or confidential reporting. Employees must fully understand how these channels operate, how they should be used, and how they will be protected to have the confidence to use them. Policies and procedures exist requiring all communication through these channels to be assessed, prioritized, and investigated. Escalation procedures ensure that necessary communication will be made to a specific board member who is responsible for ensuring that timely and proper assessments, investigations, and actions are carried out.

427 These separate mechanisms, which encourage employees to report suspected violations of an entity's code of conduct without fear of reprisal, send a clear message that senior management is committed to open communication channels and will act on information that is reported to them.

Method of Communication

428 Both the clarity of the information and effectiveness with which it is communicated are important to ensuring messages are received as intended. Active forms of communication such as face-to-face meetings are often more effective than passive forms such as broadcast emails and intranet postings. Periodic evaluation of the effectiveness of communication helps to ensure methods are working. This can be done through a variety of existing processes such as employee performance evaluations, annual management reviews, and other feedback programs.

429 Management selects the method of communication, taking into account the audience, nature of the communication, timeliness, cost, and any legal or regulatory requirements. Communication can take such forms as:

- Dashboards
- Email messages
- Live or online training
- Memoranda
- One-on-one discussions
- Performance evaluations
- Policies and procedures
- Presentations
- Social media postings
- Text messages
- Webcast and other video forms
- Website or collaboration site postings

430 When choosing a method of communication, management considers the following:

- Where messages are transmitted orally—in large groups, smaller meetings, or one-on-one sessions—the person's tone of voice and non-verbal cues emphasize what is being said and enhance understanding and opportunity for recipients to respond to the communication.
- Cultural, ethnic, and generational differences can affect how messages are received and should be considered in the method of communication to support a variety of audiences (e.g., by translating messages into multiple languages, holding one-to-one meetings that respect a preference for privacy in certain matters, and the use of technology-based media).

- Communications directly relevant to internal control effectiveness may require a method that allows for long-term retention. In some instances, employee acknowledgment of review and understanding of certain policies should be retained (e.g., code of conduct, anti-money laundering, and corporate security).
- Time-sensitive communications delivered through informal methods such as email, text messaging, and social media postings may be sufficient and more cost-effective, particularly when confidentiality or retention is not necessary.
- Management and personnel that communicate solely through formal means (e.g., official office memos) may not reach their intended audience and may not receive return communications from those who are more comfortable using informal means of communication (e.g., email, text messages or social media postings).

431 Communication of information related to internal control responsibilities alone may not be sufficient to ensure that management and other personnel receive and respond as intended. Consistent and timely actions taken by management with such communication reinforce the messages conveyed.

Communicates Externally

Principle 15: The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.

Points of Focus

432 The following points of focus may assist management in determining whether this principle is present and functioning:

- **Communicates to External Parties**—Processes are in place to communicate relevant and timely information to external parties including shareholders, partners, owners, regulators, customers, and financial analysts and other external parties.
- **Enables Inbound Communications**—Open communication channels allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others, providing management and the board of directors with relevant information.
- **Communicates with the Board of Directors**—Relevant information resulting from assessments conducted by external parties is communicated to the board of directors.
- **Provides Separate Communication Lines**—Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.
- **Selects Relevant Method of Communication**—The method of communication considers the timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations.

Outbound Communication

433 Communication occurs not only within the entity, but with those outside as well. With open two-way external communication channels, important information concerning the entity's objectives may be obtained from and provided to shareholders or other owners, business partners, customers, regulators, financial analysts, government entities, and other external parties. Outbound communication should be viewed distinctly from external reporting as discussed in Chapter 2 Objectives, Components, and Principles.

434 The organization develops and implements controls that facilitate external communication. These may include policies and procedures to obtain or receive information from external parties and to share that information internally, allowing management and other personnel to identify trends, events, or circumstances that may impact the achievement of objectives. For example, soliciting customer input on the design or quality of products or services may enable an entity to address evolving customer demands or preferences. Alternatively, customer or supplier complaints or inquiries about shipments, receipts, billings, or other unusual activities may indicate operating problems, fraudulent activities, or errors.

435 Communication to external parties allows them to readily understand events, activities, or other circumstances that may affect how they interact with the entity. Management's communication to external parties sends a message about the importance of internal control in the organization by demonstrating open lines of communication. Communication to external suppliers and customers supports the entity's ability to maintain an appropriate control environment. Suppliers and customers need to fully understand the entity's values and cultures. They are informed of the entity's code of conduct and recognize their responsibilities in helping to ensure compliance with the code of conduct. For example, management communicates its controls relating to business dealings with vendors upon approval of a new vendor and requires the vendor to acknowledge its adherence prior to the approval of an initial purchase order with the vendor.

436 Technology and communication tools enable external parties to have access to public forums to post and discuss an entity's business, activities, and controls. When an organization uses, or authorizes its employees to use public forums, such as social media and similar unrestricted communication tools, management develops and implements controls that guide expectations for proper use to avoid jeopardizing the entity's objectives.

Inbound Communication to Management and the Board

437 Communications from external parties may also provide important information on the functioning of the entity's internal control system. These can include:

- An independent assessment of internal controls at an outsourced service provider related to the organization's objectives
- An independent auditor's assessment of internal control over financial or non-financial reporting of the entity

- Customer feedback related to product quality, improper charges, and missing or erroneous receipts
- New or changed laws, rules, regulations, standards, and other requirements of standard- and rule-setting bodies
- Results from regulatory compliance reviews or examinations such as banking, securities, or taxing authorities
- Vendor questions related to timely or missing payments for goods sold
- Postings on organization-sponsored or supported social media websites or communication tools

438 Information resulting from external assessments about the organization's activities that relate to matters of internal control are evaluated by management and, where appropriate, communicated to the board of directors. For example, management has entered into an arrangement that allows the organization to periodically use externally managed technology services to perform transaction processing in lieu of hiring personnel and purchasing and implementing additional hardware and software internally. The organization uses sensitive customer data in certain processes. To maintain compliance with the entity's policies and external laws, regulations, and standards, an assessment of internal control over the security and privacy of externally transmitted data (including data transmitted over the Internet) is performed by a third party. The results of the assessment reveal weaknesses in internal control that could impact the security and privacy of data. Management assesses the significance of the weaknesses and reports information necessary to enable the board of directors to carry out its oversight responsibilities.

439 The interdependence of business processes between the entity and outsourced service providers can blur the lines of responsibility between the entity's internal control system and that of outsourced service providers. This creates a need for more rigorous controls over communication between the parties. For example, supply chain management in a global retail company occurs through a dynamic, interactive exchange of activities between the company, vendors, logistics providers, and contract manufacturers. Internal control over the end-to-end processes becomes a shared responsibility, but there may be uncertainty about which entity is responsible at a particular stage of the process. Communicating with outsourced service providers responsible for activities supporting the entity's objectives may facilitate the risk assessment process, the oversight of business activities, decision making, and the identification of responsibility for internal control throughout the process regardless of where activities occur.

Communication beyond Normal Channels

440 Complexity of business relationships between the entity and external parties may arise through service provider and other outsourcing arrangements, joint ventures and alliances, and other transactions that create mutual dependencies between the parties. Such complexity may create concerns over how business is being conducted by or between the parties. In this case, the organization makes separate communication channels available to customers, suppliers, and outsourced service providers to allow them to communicate directly with management and other personnel. For example,

a customer of products developed through a joint venture may learn that one of the joint venture partners sold products in a country that was not agreed to under the joint venture arrangement. Such a breach may affect the customer's ability to use or resell the products, impacting the customer's business. The customer needs a channel in which it can communicate concerns to others in the organization without disrupting its ongoing operations.

Method of Communication

441 The means by which management communicates externally affects the ability to obtain information needed as well as to ensure that key messages about the organization are received and understood. Management considers the method of communication used, which can take many forms, taking into account the audience, the nature of the communication, timeliness, and any legal or regulatory requirements. For example, customers who regularly access entity information through a customer portal may receive messages through postings on the corporate website.

442 Press and news releases issued through investor or public relations channels are often effective for reaching a broad audience of external parties, ensuring wide distribution and increasing the likelihood that information is received. Blogs, social media, electronic billboards, and email are also common forms of external communication because they can be tailored and directed to the specific party, help to control the information obtained by external parties, and support expectations that information can be sent and received quickly with greater use of mobile communication devices.

9. Monitoring Activities

Chapter Summary

443 Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to effect the principles within each component, is present and functioning. Ongoing evaluations, built into business processes at different levels of the entity, provide timely information. Separate evaluations, conducted periodically, will vary in scope and frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations. Findings are evaluated against criteria established by regulators, standard-setting bodies, or management and board of directors, and deficiencies are communicated to management and the board of directors as appropriate.

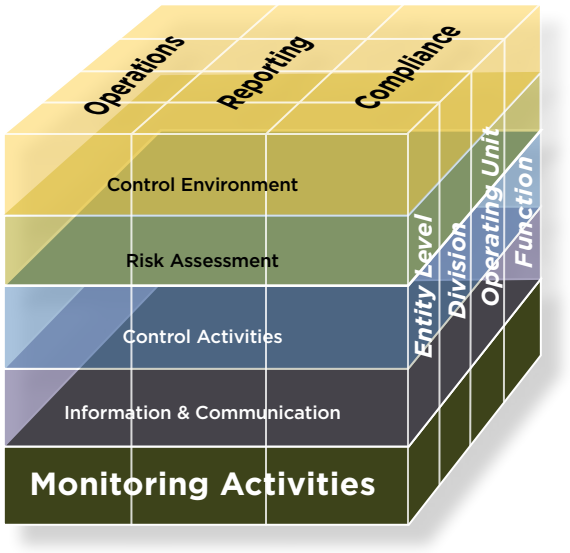
Principles relating to the Monitoring Activities component

16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Introduction

444 Monitoring activities assess whether each of the five components of internal control is present and functioning. The organization uses ongoing, separate evaluations, or some combination of the two, to ascertain whether the components of internal control (including controls to effect principles across the entity and its subunits) are present and functioning. Monitoring is a key input into the organization's assessment of the effectiveness of internal control. It provides valuable support for assertions, if required, regarding the effectiveness of the system of internal control.



445 An entity's system of internal control will often change. The entity's objectives and the components of internal control may also change over time. Also, procedures may become less effective or obsolete, may no longer be in place and functioning, or may be deemed insufficient to support the achievement of the new or updated objectives. Monitoring activities are selected, developed, and performed to ascertain whether each component continues to be present and functioning or if change is needed. When a component or a principle drawn from the five components is not present and functioning, some form of internal control deficiency exists. Management also needs to determine whether the system of internal control continues to be relevant and is able to address new risks.

446 Where appropriate, monitoring activities identify and examine expectation gaps relating to anomalies and abnormalities, which may indicate one or more deficiencies in an entity's system of internal control. In reviewing and investigating expectation gaps management often identifies root causes of such gaps.

447 When distinguishing between a monitoring activity and a control activity, organizations need to consider underlying details of the activity in determining whether an activity is a control activity versus a monitoring activity, especially where the activity involves some level of supervisory review. Supervisory reviews are not automatically classified as monitoring activities and it may be a matter of judgment whether a review is classified as a control activity or a monitoring activity. For example, the intent of a monthly completeness control activity would be to detect and correct errors, where a monitoring activity would ask why there were errors in the first place and assign management the responsibility of fixing the process to prevent future errors. In simple terms, a control activity responds to a specific risk, whereas a monitoring activity assesses whether controls within each of the five components of internal control are operating as intended, among other things.

448 The examples below illustrate the relationship between control activities and monitoring activities of a payable reconciliation.

Control Activities	Monitoring Activities
• The accounts payable (AP) clerk at Division A reconciles the Division A payables sub-ledger to the general ledger on a periodic basis. Reconciling items are investigated and resolved on a timely basis.	• Management independent of those involved in the performance of the control activity: - Inspects documentation that the reconciliations were performed across all divisions or subsidiaries. - Examines for identifiable trends in the volume and/or nature of the reconciling items noted. • Management evaluates whether the sources and the quality of information used for the payable reconciliation are appropriate. • Management evaluates whether new risks relating to changes in internal and external factors were identified, assessed, and responded to in the payables reconciliation.
• The AP supervisor periodically reviews and approves the payables sub-ledger to general ledger account reconciliation.	• Semiannually, management evaluates whether supervisors performing the review and approval are properly trained and knowledgeable.

Conducts Ongoing and/or Separate Evaluations

Principle 16: The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

Points of Focus

449 The following points of focus may assist management in determining whether this principle is present and functioning:

- **Considers a Mix of Ongoing and Separate Evaluations**—Management includes a balance of ongoing and separate evaluations.
- **Considers Rate of Change**—Management considers the rate of change in business and business processes when selecting and developing ongoing and separate evaluations.
- **Establishes Baseline Understanding**—The design and current state of an internal control system are used to establish a baseline for ongoing and separate evaluations.
- **Uses Knowledgeable Personnel**—Evaluators performing ongoing and separate evaluations have sufficient knowledge to understand what is being evaluated.
- **Integrates with Business Processes**—Ongoing evaluations are built into the business processes and adjust to changing conditions.
- **Adjusts Scope and Frequency**—Management varies the scope and frequency of separate evaluations depending on risk.
- **Objectively Evaluates**—Separate evaluations are performed periodically to provide objective feedback.

Ongoing and Separate Evaluations

450 Monitoring can be done in two ways: through ongoing evaluations or separate evaluations, or some combination of the two. Ongoing evaluations are generally defined, routine operations, built in to business processes and performed on a real-time basis, reacting to changing conditions. Where ongoing evaluations are built in to business processes, the components of internal control are usually structured to monitor themselves on an ongoing basis, at least to some degree. Separate evaluations are conducted periodically by objective management personnel, internal audit, and/or external parties, among others. The scope and frequency of separate evaluations is a matter of management judgment.

451 Since separate evaluations take place periodically, problems will often be identified more quickly by ongoing evaluations. Many entities with sound ongoing evaluations will nonetheless conduct separate evaluations of the components of internal control to reconfirm ongoing evaluation conclusions. An entity that perceives a need for frequent separate evaluations may consider identifying ways to enhance ongoing evaluations.

452 Management selects, develops, and performs a mix of monitoring activities usually including both ongoing and separate evaluations, to ascertain whether each of the five components of internal control are present and functioning. As part of monitoring the five components, management uses these evaluations to ascertain whether controls to effect principles across the entity and its subunits have been designed, implemented, and conducted. The decision of whether to conduct ongoing or separate evaluations, or some combination of the two, may occur at different levels of the entity. Thought is given to the scope and nature of the entity's operations, changes in internal and external factors, and the associated risks when developing the ongoing and separate evaluations.

Rate of Change

453 Management considers the rate that an entity or the entity's industry is anticipated to change. An entity in an industry that is quickly changing may need to have more frequent separate evaluations and may reconsider the mix of ongoing and separate evaluations during the period of change. For example, banks subject to financial regulatory reforms select and develop monitoring activities that anticipate future change and reactions to the changing regulatory environment. Usually, some combination of ongoing and separate evaluations will validate whether or not the components of internal control remain present and functioning.

454 Monitoring activities may be used to support external reporting including management assertions over the entity's system of internal control or other forms of compliance reporting. The requirements of external reporting or management assertions will usually affect the combination of ongoing and separate evaluations and how they are selected, developed, and performed.

Baseline Information

455 Understanding the design and current state of a system of internal control system provides useful baseline information for establishing ongoing and separate evaluations.

456 Monitoring activities require an understanding of how management has designed the system of internal control and how controls have been designed, implemented, and conducted. As management gains experience with monitoring activities, its baseline understanding will evolve based on the results of such activities. If an entity does not have a baseline understanding in areas with risks of higher significance, it may need to perform a separate evaluation of those areas to establish the baseline. When change occurs within the components of internal control, the baseline may need to be evaluated to make sure monitoring activities remain appropriate or updated so they are aligned with other components of internal control.

Ongoing Evaluations

457 Manual and automated ongoing evaluations monitor the presence and functioning of the components of internal control in the ordinary course of managing the business. Ongoing evaluations are generally performed by line operating or functional managers, who are competent and have sufficient knowledge to understand what is being evaluated, giving thoughtful consideration to implications of information they receive. By focusing on relationships, inconsistencies, or other relevant implications, they raise issues and follow up with other personnel as necessary to determine whether corrective or other action is needed.

458 Entities frequently use technology to support control activities and monitor the components of internal control. Technology offers an opportunity to use computerized monitoring, which has a very high standard of objectivity (once programmed and tested) and allows for efficient review of large volumes of data at a low cost. Advances in automated activities have made continuous monitoring computer applications available, and these should be considered when selecting ongoing evaluations.

459 The following examples illustrate ongoing evaluations.

The quality officer of a medium-size manufacturing company participates in a monthly production meeting where she obtains information regarding approval of product modifications. The quality officer review raises probing questions to identify unusual trends or anomalies, may initiate investigations, and may use information obtained from the investigations to modify control activities that authorize other personnel to alter production terms.

An entity uses software to automate the review of all payment transactions. This software identifies unusual transactions within the payable business process, including the identification of possible duplicate payments, based on pre-established parameters. Identified anomalies are investigated to determine the root cause, and any internal control deficiencies are identified, reported, and appropriately acted on.

The chief compliance officer, as part of his review of the monthly reporting process to the board reviews, reports from the entity's hotline process for trends, and makes direct inquiries into any increased activity.

An entity allows a contract management variance of 5% in paying contractors. The contract payments are reviewed quarterly to determine if any staff are routinely approving within the 5% variance, since the 5% should be an exception and not routine. Identified exceptions are investigated to determine if there are any internal control deficiencies. If deficiencies are found, they are reported to determine if adjustments to the process are necessary.

Separate Evaluations

460 Separate evaluations are generally not ingrained within the business but can be useful in taking a fresh look at whether each of the five components of internal control are present and functioning. Such evaluations include observations, inquiries, reviews, and other examinations, as appropriate, to ascertain whether controls to effect principles across the entity and its subunits, are designed, implemented, and conducted. Separate evaluations of the components of internal control vary in scope and frequency, depending on the significance of risks, risk responses, results on ongoing evaluations, and expected impacts on the control components in managing the risks. Higher priority risks and responses should be evaluated often in greater depth and/or more often than lower priority risks. While higher priority risks can be evaluated with both ongoing and separate evaluations, separate evaluation may provide feedback on the results of ongoing evaluations, and the number of separate evaluations can be increased as necessary.

461 A separate evaluation of the overall internal control system, or specific components of internal control, may be appropriate for a number of reasons: major strategy or management change, acquisitions or dispositions, changes in economic or political conditions, or changes in operations or methods of processing information. The evaluation scope is determined by which of the three objectives categories—operations, reporting, or compliance—are being addressed.

Knowledgeable Personnel

462 Separate evaluations are often conducted through the internal audit function, and while having an internal audit function is not a requisite of internal control, it can enhance the scope, frequency, and objectivity of such reviews.[21] Since separate evaluations are conducted periodically by independent managers, employees, or external reviewers to provide feedback with greater objectivity, evaluators need to be knowledgeable about the entity's activities and how the monitoring activities function, and understand what is being evaluated. Procedures designed to operate in a particular way may be modified over time to operate differently, or they may no longer be performed. Sometimes new procedures are established, but are not known to those who described the process and are not included in available documentation. Determining the actual functioning can be accomplished by holding discussions with personnel who perform or are affected by controls, by examining performance records, or by a combination of procedures.

463 The evaluator analyzes the components of internal control design and operation, and the results of evaluations. The analysis is conducted against the backdrop of management's established standards for each component, with the ultimate goal of determining whether the process provides reasonable assurance with respect to the stated objectives.

21 Some external bodies may require an entity to have an internal audit function. For example the New York Stock Exchange requires all corporations who list securities on the exchange to have an internal audit function (NYSE Listed Company Manual 303A.07(d)).

Separate Evaluation Approaches and Objectivity

464 There are a variety of approaches available to perform separate evaluations. The scope, nature, frequency, and formality of approaches vary with the relative importance of the risk responses and related components and principles of internal control that are being evaluated. Separate evaluations may include:

- *Internal Audit Evaluations*—Internal auditors are often objective and competent resources, whether in-house or outsourced, and perform separate evaluations as part of their regular duties, or at the specific request of senior management or the board of directors. For example, each year the internal audit function develops an internal audit plan of projects that are selected based on a risk-based approach aligned with organizational objectives and stakeholder priorities. Reports are distributed to senior management, the board of directors or its audit committee, and to other parties positioned to take action on the recommendations in the report.
- *Other Objective Evaluations*—For entities that lack an internal audit group or for those that have other quality functions that perform internal audit-like activities (such as a controls compliance group), management may use other internal or external objective reviewers, such as compliance officers, operations specialists, IT security specialists, or consultants. For example, an entity's IT security specialist may periodically evaluate the entity's compliance with ISO/IEC 27002 Information Security Standard.
- *Cross Operating Unit or Functional Evaluations*—An entity may use personnel from different operating units or functional areas to evaluate components of internal controls. For example, quality audit personnel from operating unit A may periodically evaluate the internal controls of operating unit B. Also, adding personnel from different operating units or functional areas on evaluations may improve communications between the operating unit or functional area.
- *Benchmarking/Peer Evaluations*—Some entities compare or benchmark components of internal control against those of other entities. Such comparisons might be done directly with another entity or under the auspices of trade or industry associations. Other entities may be able to provide comparative information. A word of caution: when conducting comparisons, consider the differences that always exist in objectives, facts, and circumstances.
- *Self-Assessments*—Separate evaluations may take the form of self-assessments (also called self-reviews), where those responsible for a particular unit or function will assess the presence and functioning of components of internal control relating to their activities. For example, in one company the chief executive of a food product division directs the evaluation of its internal control activities related to food safety regulations. She personally assesses the controls associated with strategic choices and high-level objectives as well as the components of internal environment, and individuals in charge of the division's various operating activities assess the presence and functioning of internal components relative to their spheres of responsibility. Since self-assessments have less objectivity than other separate evaluation approaches, the evaluator or those using the report will determine the weight and value to be placed on the results.

Outsourced Service Providers

465 Entities that use outsourced service providers for services such as third-party warehousing, Internet hosting, healthcare claims processing, retirement plan administration, or loan services need to understand the activities and controls associated with the services and how the outsourced service provider's internal control system impacts the entity's system of internal control.

466 Entities may use the following approaches to gain an understanding of the outsourced service provider's system of internal control since the type of information required to monitor outsourced service providers varies:

- The user of outsourced services may conduct its own separate evaluations of the outsourced service provider's system of internal control as relevant to the entity. In these circumstances an entity should build into its contract with any outsourced service provider a right-to-audit clause to allow for its own separate evaluation and access to visit the provider.
- Relevant information concerning internal control at an outsourced service provider may be attained by reviewing an independent audit or examination report.[22] When reviewing such reports, organizations consider the content of the assertions and attestations to be satisfied that the outsourced service provider's controls interface with the entity's controls, and that the tests and results of the outsourced service provider's controls provide sufficient comfort to the user entity. Entities also consider the period of time covered by independent audit or examination report since it might not coincide with or provide the complete coverage needed by the entity. In these circumstances an entity should build into its contract with any outsourced service provide a requirement for an independent audit or examination report.
- When considering circumstances such as the nature and scope of information transferred between parties and the nature of the processing and reporting the outsourced service provider performs, an entity may be able to determine that there is sufficient internal control over processing provided by the outsourced service provider without additional documentation.

22 Examples of attestations for external financial reporting include a Service Organization Control (SOC) report issued pursuant to the AICPA's Statement on Standards for Attestation Engagements No 16 (SSAE 16 or SOC 1) or the International Standard on Assurance Engagements 3402 report (ISAE 3402).

Evaluates and Communicates Deficiencies

Principle 17: The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Points of Focus

467 The following points of focus may assist management in determining whether this principle is present and functioning:

- **Assesses Results**—Management and the board of directors, as appropriate, assess results of ongoing and separate evaluations.
- **Communicates Deficiencies**—Deficiencies are communicated to parties responsible for taking corrective action and to senior management and the board of directors, as appropriate.[23]
- **Monitors Corrective Actions**—Management tracks whether deficiencies are remediated on a timely basis.

Assess Results

468 In conducting monitoring activities, the organization may identify matters worthy of attention. Those that represent a potential or real shortcoming in some aspect of the system of internal control that has the potential to adversely affect the ability of the entity to achieve its objectives are referred to as deficiencies. In addition, the organization may identify opportunities to improve the efficiency of internal control, or areas where changes to the current system of internal control may provide a greater likelihood that the entity's objectives will be achieved. Although identifying and assessing potential opportunities is not part of the system of internal control, the organization will typically want to capture any opportunities identified and communicate those to the strategy or objective-setting processes.

469 Deficiencies in an entity's components of internal control and underlying principles may surface from a variety of sources:

23 In many cases the board of directors will appoint a committee or committees to oversee the system of internal control, depending on the objective. For example, the board may appoint an audit committee to oversee system of internal controls for financial reporting.

- Monitoring activities, including:
  - Ongoing evaluations of an entity, including managerial activities and everyday supervision of employees, generate insights from those who are directly involved in the entity's activities. These insights are obtained in real time and can quickly identify deficiencies.
  - Separate evaluations performed by management, internal auditors, functional managers, and other personnel can highlight areas that need to be improved.
- Other components of internal control provide input relative to the operation of that component.
- External parties such as customers, vendors, external auditors, and regulators frequently provide important information about an entity's components of internal control.

Communicating Internal Control Deficiencies

470 Reporting on internal control deficiencies depends on the criteria established by regulators, standard-setting bodies, and management and board of directors, as appropriate. Results of ongoing and separate evaluations are assessed against those criteria to determine to whom to report and what is reported. Management's criteria is typically based on the entity's facts and circumstances and on established laws, rules, regulations, and standards,

471 Communicating internal control deficiencies to the right parties to take corrective actions is critical for entities to achieve objectives. Additionally, the scope and approach of the evaluations, as well as any internal control deficiencies, need to be communicated to those conducting the overall assessment of effectiveness of internal control.

472 The nature of matters to be communicated varies depending on how the deficiency is evaluated against appropriate criteria, individuals' authority to deal with circumstances that arise, and the oversight activities of superiors. Deficiencies may be reported to senior management and the board of directors depending on the reporting criteria as established by regulators, standard-setting bodies, or the entity, as appropriate. After deficiencies are evaluated management tracks whether remediation efforts are conducted on a timely basis. Internal control deficiencies are usually reported both to the parties responsible for taking corrective action and to at least one level of management above that person.

473 This higher level of management provides needed support or oversight for taking corrective action and is positioned to communicate with others in the entity whose activities may be affected. Where findings cut across organizational boundaries, the deficiencies are reported to all relevant parties and to a sufficiently high level to drive appropriate action. For instance, deficiencies relating to the board of directors where the board is not independent to the extent required, or where the board did not provide sufficient oversight, would be reported as prescribed by the entity's reporting protocols to the full board, the chair of the board, lead director, and/or the nominating/governance or other appropriate board committees.

474 In considering what needs to be communicated, it is necessary to look at the implications of findings and the entity's reporting directives. It is essential that not only a particular transaction or event be reported, but also that related faulty procedures be re-evaluated. Alternative communications channels should also exist for reporting sensitive information such as illegal or improper acts. Additionally, deficiencies may need to be reported externally depending on the type of entity and the regulatory, industry, or other compliance requirements to which it is subject.

10. Limitations of Internal Control

Chapter Summary

475 Internal control, no matter how well designed, implemented and conducted, can provide only reasonable assurance to management and the board of directors of the achievement of an entity's objectives. The likelihood of achievement is affected by limitations inherent in all systems of internal control. These include the realities that human judgment in decision making can be faulty and that breakdowns can occur because of human failures such as making errors. Additionally, controls can be circumvented by two or more people colluding, and because management can override the internal control system.

476 Internal control has been viewed by some observers as ensuring that an entity will not fail—that is, the entity will always achieve its operations, reporting, and compliance objectives. In this sense, internal control sometimes is looked upon as a cure-all for all real and potential business ills. This view is misguided. Internal control is not a panacea.

477 In considering limitations of internal control, two distinct concepts must be recognized. First, internal control, even effective internal control, operates at different levels for different objectives. For objectives relating to the effectiveness and efficiency of an entity's operations—achieving its mission, value propositions (e.g., productivity, quality, and customer service), profitability goals, and the like—internal control may not necessarily provide reasonable assurance of the achievement of that objective unless based on external standard exists. Otherwise, internal control can only provide reasonable assurance that the organization is aware of the entity's progress, or lack of thereof, toward achieving such objectives. When an external standard does not exist to specify suitable objectives, internal control cannot provide absolute assurance that the objectives categories can be achieved.

478 The first set of limitations acknowledges that certain events or conditions are simply outside management's control. The second acknowledges that no system of internal control will always do what it is designed to do. The best that can be expected in any of system of internal control is that reasonable assurance be obtained, which is the focus of this chapter.

479 Reasonable assurance does not imply that systems of internal control will frequently fail. Many factors, individually and collectively, serve to strengthen the concept of reasonable assurance. Controls that satisfy multiple objectives and the multipurpose nature of many controls reduce the risk that an entity may not achieve its objectives. Furthermore, the normal, everyday operating activities and responsibilities of people functioning at various levels of an organization are directed at achieving the entity's objectives. Indeed, it is likely that these activities often apprise management about the process toward the entity's operations objectives, and also support the achievement of compliance and reporting objectives. However, because of the inherent limitations discussed above, there is no guarantee that, for example, an uncontrollable event, mistake, or improper incident could never occur. In other words, even an effective system of internal control may experience failures. Reasonable assurance is not absolute assurance.

Preconditions of Internal Control

480 The Framework specifies several areas that are part of the management process but not part of internal control. Two such areas relate to establishing objectives as a pre-condition to internal control and to parts of the governance process that extend the board's role beyond internal control. There is a dependency established on these areas, among others, to also be effective. An entity's weak governance processes for selecting, developing, and evaluating board members may limit its ability to provide appropriate oversight of internal control. Similarly, ineffective strategy-setting or objective-setting processes would challenge the entity's ability to identify poorly specified, unrealistic, or unsuitable objectives. A system of internal control cannot encompass all activities undertaken by the entity, and weaknesses in these areas may impede the organization in having effective internal control.

Judgment

481 The effectiveness of internal control is limited by the realities of human frailty in the making of business decisions. Such decisions must be made with human judgment in the time available, based on information at hand, and under the pressures of the conduct of business. Some decisions based on human judgment may later, with the clarity of hindsight, be found to produce less than desirable results, and may need to be changed.

Breakdowns

482 Even a well-designed system of internal control can break down. Personnel may misunderstand instructions, make mistakes in judgment, or commit errors due to carelessness, distraction, or being asked to focus on too many tasks. For example, a department supervisor responsible for investigating exceptions might simply forget or fail to pursue the investigation far enough to be able to make appropriate corrections. Temporary personnel conducting controls for vacationing or sick employees might not perform correctly. Changes in the design of information technology application controls may be implemented before personnel have been trained to indicators that it may not be functioning as designed.

Management Override

483 Even an entity with an effective system of internal control may have a manager who is willing and able to override internal control. The term "management override" is used here to mean overruling prescribed policies or procedures for illegitimate purposes with the intent of personal gain or an enhanced presentation of an entity's performance or compliance. A manager of a division or operating unit, or a member of senior management, might override the control for many reasons such as to:

- Increase reported revenue to cover an unanticipated decrease in market share
- Enhance reported earnings to meet unrealistic budgets
- Boost the market value of the entity prior to a public offering or sale
- Meet sales or earnings projections to bolster bonus payouts tied to performance
- Appear to cover violations of debt covenant agreements
- Hide lack of compliance with legal requirements

484 Override practices include deliberately making misrepresentations to bankers, lawyers, accountants, and vendors, and intentionally issuing false documents such as purchase orders and sales invoices.

485 Management override should not be confused with management intervention, which represents management's actions to depart from prescribed controls for legitimate purposes. Management intervention is necessary to deal with non-recurring and non-standard transactions or events that otherwise might be handled inappropriately. Provision

for management intervention is necessary because no process can be designed to anticipate every risk and every condition. Management's actions to intervene are generally overt and commonly documented or otherwise disclosed to appropriate personnel. Actions to override usually are not documented or disclosed, and have the intent to cover up the actions.

Collusion

486 Collusion can result in internal control deficiencies. Individuals acting collectively to perpetrate and conceal an action from detection often can alter financial or other management information so that it cannot be detected or prevented by the system of internal control. Collusion can occur, for example, between an employee who performs controls and a customer, supplier, or another employee, Sales and/or operating unit management might collude to circumvent controls so that reported results meet budgets or incentive targets.

Appendices

A. Glossary

- **Application Controls**—Programmed procedures in application software and related manual procedures designed to help ensure the completeness and accuracy of information processing.
- **Automated Controls**—Control activities mostly or wholly performed through technology (e.g., automated control functions programmed into computer software; contrast with **Manual Controls**).
- **Board**—Governing body of an entity, which may take the form of a board of directors or supervisory board for a corporation, board of trustees for a not-for-profit organization, board of governors or commissioners for government entities, general partners for a partnership, or owner for a small business.
- **Category**—One of three groupings of objectives of internal control. The categories relate to operations, reporting, and compliance.
- **Compliance**—Having to do with conforming with laws and regulations applicable to an entity.
- **Component**—One of five elements of internal control. The internal control components are the Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities.
- **Control**—**(1)** A noun (i.e., existence of a control), a policy or procedure that is part of internal control. Controls exist within each of the five components. **(2)** A verb (i.e., to control), to establish or implement a policy or procedure that effects a principle.
- **Control Activity**—An action established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.
- **Control Deficiency**—A synonym for **Internal Control Deficiency**. A control deficiency may also describe a deficiency with respect to a particular control or control activity.
- **COSO**—The Committee of Sponsoring Organizations of the Treadway Commission. COSO is a joint initiative of five private-sector organizations that are dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control. and fraud deterrence (see www.coso.org).
- **Design**—**(1)** Intent; as used in the definition of internal control, the internal control system design is intended to provide reasonable assurance of the achievement of objectives; when the intent is realized, the system can be deemed effective. **(2)** Plan; the way a system is supposed to work, contrasted with how it actually works.
- **Detective Control**—A control designed to discover an unintended event or result after the initial processing has occurred but before the ultimate objective has concluded (contrast with **Preventive Control**).

- **Effected**—Used with an internal control system: devised and maintained.
- **Effective Internal Control**—Internal control that is judged to be effective resulting from an assessment of whether each of the five components of internal control is present and functioning, and whether the five components of internal control are operating together.
- **Effective Internal Control System**—A synonym for **Effective Internal Control**.
- **Entity**—A legal entity or management operating model of any size established for a particular purpose. A legal entity may, for example, be a business enterprise, not-for-profit organization, government body, or academic institution. The management operating model may follow product or service lines, division, or operating unit, with geographic markets providing for further subdivisions or aggregations of performance.
- **Entity-level**—Higher levels of the entity, separate and distinct from other parts of the entity including subsidiaries, divisions, operating units, and functions.
- **Entity-wide**—Activities that apply across the entity—most commonly in relation to entity-wide controls.
- **Ethical Values**—Moral values that enable a decision-maker to determine an appropriate course of behavior; these values should be based on what is right, which may go beyond what is legal.
- **Financial Statements**—Typically a statement of financial position, a statement of income, a statement of changes in equity, a statement of cash flow, and notes to the financial statements.
- **Inherent Limitations**—Those limitations of all internal control systems. The limitations relate to the preconditions of internal control, limits of human judgment, the reality that breakdowns can occur, and the possibility of management override and collusion.
- **Integrity**—The quality or state of being of sound moral principle; uprightness, honesty, and sincerity; the desire to do the right thing, to profess and live up to a set of values and expectations.
- **Internal Control**—A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.
- **Internal Control Deficiency**—A shortcoming in the system of internal control, component, or principle that has the potential to affect the ability of the entity to achieve its objectives.
- **Management Override**—Management's overruling of prescribed policies or procedures for illegitimate purposes with the intent of personal gain or an enhanced presentation of an entity's financial condition or compliance status.
- **Management Process**—The series of actions taken by management to run an entity. An internal control system is a part of and integrated with the management process.

- **Manual Controls**—Controls performed manually, not through technology (contrast with **Automated Controls**).
- **Operations**—Used with "objectives" or "controls": having to do with the effectiveness and efficiency of an entity's operations, including performance and profitability goals, and safeguarding resources.
- **Organization**—People, including the board of directors, senior management, and other personnel.
- **Policy**—Management or board member statement of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. A policy serves as the basis for procedures.
- **Present and Functioning**—Applied to components and principles. "Present" refers to the determination that components and relevant principles are reflected in the design and implementation of the system of internal control. "Functioning" refers to the determination that components and relevant principles have been reflected in the conduct of the organization.
- **Preventive Control**—A control designed to avoid an unintended event or result at the time of initial occurrence (contrast with **Detective Control**).
- **Procedure**—An action that implements a policy.
- **Published Financial Statements**—Financial statements, interim and condensed financial statements, and selected data derived from such statements, and reported publicly.
- **Reasonable Assurance**—The concept that internal control, no matter how well designed and operated, cannot guarantee that an entity's objectives will be met. This is because of **Inherent Limitations** in all internal control systems.
- **Risk**—The possibility that an event will occur and adversely affect the achievement of objectives.
- **Risk Response**—The decision to accept, avoid, reduce, or share a risk.
- **Risk Tolerance**—The acceptable variation relative to performance to the achievement of objectives.
- **Senior Management**—The chief executive officer or equivalent organizational leader and senior management team.
- **Stakeholders**—Parties that are affected by the entity, such as shareholders, the communities in which an entity operates, employees, customers, and suppliers.
- **Technology**—Software applications running on a computer, manufacturing controls systems, etc.

- **Technology General Controls**—Control activities that help ensure the continued, proper operation of technology. They include controls over the technology infrastructure, security management, and technology acquisition, development, and maintenance. Other terms sometimes used to describe technology general controls are "general computer controls" and "information technology controls."
- **Transaction Controls**—Control activities that directly support the actions to mitigate transaction processing risks in an entity's business processes. Transaction controls can be manual or automated and will likely cover the information-processing objectives of completeness, accuracy, and validity.

B. Roles and Responsibilities

Introduction

487 Internal control is effected by personnel internal to the organization, including the board of directors or equivalent oversight body and its committees, management and personnel, business-enabling functions, and internal auditors. Collectively, they contribute to providing reasonable assurance that specified objectives are achieved. When outsourced service providers perform controls on behalf of the entity, management retains responsibility for those controls.

488 An organization may view internal control through three lines of defense:

- Management and other personnel on the front line provide the first line of defense as they are responsible for maintaining effective internal control day to day; they are compensated based on performance in relation to all applicable objectives.
- Business-enabling functions such as risk, control, legal, and compliance provide the second line of defense as they clarify internal control requirements and evaluate adherence to defined standards. While they are functionally aligned to the business, their compensation is not directly tied to performance of the area to which they render expert advice.
- Internal auditors provide the third line of defense as they assess and report on internal control and recommend corrective actions or enhancements for management to consider and implement; their position and compensation are separate and distinct from the business areas they review.

489 Parties external to the organization, such as customers, vendors, and outsourced service providers, may perform controls or provide information useful for conducting internal control. The entity may audit any outsourced service provider's adherence to contractual obligations, which may include standards of conduct, standards of performance, and required communications. The entity may also assess the underlying controls, including controls over the quality of data and information provided by the entity to the outsourced service provider, the provider's controls over processing of that data and information, and the reasonableness of the outputs from that processing. However, these outsourced service providers are not responsible for the entity's system of internal control.

Responsible Parties

490 Every individual within an entity has a role in effecting internal control. Roles vary in responsibility and level of involvement, as discussed below.

The Board of Directors and Its Committees

491 Depending on the jurisdiction and nature of the organization, different governance structures may be established, such as a board of directors, supervisory board, trustees, and/or general partners, with committees as appropriate. In the Framework, these governance structures are commonly referred to as the board of directors.

492 The board is responsible for overseeing the system of internal control. With the power to engage or terminate the chief executive officer, the board has a key role in defining expectations about integrity and ethical values, transparency, and accountability for the performance of internal control responsibilities. Board members are objective, capable, and inquisitive. They have a working knowledge of the entity's activities and environment, and they commit the time necessary to fulfill their governance responsibilities. They utilize resources as needed to investigate any issues, and they have an open and unrestricted communications channel with all entity personnel, the internal auditors, independent auditors, external reviewers, and legal counsel.

493 Boards of directors often carry out certain duties through committees, whose use varies depending on regulatory requirements and other considerations. Board committees may be used for oversight of audit, compensation, nominations and governance, risk, and other topics significant for the organization. Each committee can bring specific emphasis to certain components of internal control. Where a particular committee has not been established, the related functions are carried out by the board itself.

494 Board-level committees can include the following:

- *Audit Committee*—Regulatory and professional standard-setting bodies often require the use of audit committees. The role and scope of authority of an audit committee can vary depending on the organization's regulatory jurisdiction, industry norm, or other variables. This is sometimes also called the audit and risk committee to emphasize the importance of risk oversight. Management is responsible for the reliability of the financial statements, but an effective audit committee plays a critical oversight role. The board of directors, often through its audit committee, has the authority and responsibility to question senior management regarding how it is carrying out its internal and external reporting responsibilities and to verify that timely corrective actions are taken, as necessary.

  As a result of its independence the audit committee, along with a strong internal audit function as applicable, is often best positioned, to identify and promptly act in situations where senior management overrides controls or deviates from expected standards of conduct. The audit committee interacts with external auditors, meeting regularly to discuss the scope of planned audit procedures and results of audit procedures. Meetings with external auditors include executive sessions without management present to provide a forum

for further dialogue between external auditors and audit committees. While board composition requirements vary, independent directors are important as they can provide an objective perspective. For example, the UK, German, and other corporate governance codes, and the New York Stock Exchange (NYSE) and NASDAQ listing requirements define the number and criteria for audit committee members to be independent from management and financially literate (e.g., at least one member with accounting or financial management expertise).

- *Compensation Committee*—Establishes the compensation for the chief executive officer or equivalent and provides oversight of compensation arrangements to motivate without providing incentives for undue risk-taking so as to ultimately protect and promote the interest of shareholders or other owners of the entity. It oversees senior management in its role to balance performance measures, incentives, and rewards with the pressures created by the entity's objectives, and helps structure compensation practices to support the achievement of the entity's objectives without unduly emphasizing short-term results over long-term performance.
- *Nomination/Governance Committee*—Provides control over the selection of candidates for directors and senior management. It regularly assesses and nominates members of the board of directors; makes recommendations regarding the board's composition, operations, and performance; oversees the succession planning process for the chief executive officer and other key executives; and develops oversight discipline, processes, and structures. It promotes director orientations and training and evaluates oversight structures and processes (e.g., board/committee evaluations).
- *Other Committees*—There may be other committees of the board of directors that oversee specific areas. These committees are often established in large organizations or due to particular circumstances of the entity. For example, in an industry where compliance with certain laws and regulations is fundamental to the survival or development of the organization, a board-level compliance committee may be necessary. Risk committees are formed to focus on changes in risk levels and related impacts, and oversight of risk responses. Further to board committees that provide oversight, management-level committees often exist to provide guidance in the execution of specific areas, such as compliance committees, new product committees, and others.

Chief Executive Officer

495 The chief executive officer (CEO) is accountable to the board of directors and is responsible for designing, implementing, and conducting an effective system of internal control. In privately owned, not-for-profit, or other entities, the equivalent role may have a different title but generally covers the same responsibilities as described below. More than any other individual, the CEO sets the tone at the top that affects the control environment and all other components of internal control.

496 The CEO's responsibilities relating to internal control include:

- Providing leadership and direction to senior management. With the support of management, the CEO shapes entity values, standards, expectations of competence, organizational structure, and accountability that form the foundation of the entity's internal control system (e.g. specifies entity-wide objectives and policies).
- Maintaining oversight and control over the risks facing the entity (e.g., directing all management and other personnel to proactively identify risks to the system of internal control, considering the ever-increasing pace of change and networked interactions of business partners, outsourced service providers, customers, employees, and others and resulting risk factors).
- Guiding the development and performance of control activities at the entity level, and delegating to various levels of management the design, implementation, conduct, and assessment of internal control at different levels of the entity (e.g., processes and controls to be established).
- Communicating expectations (e.g., integrity, competence, key policies) and information requirements (e.g., the type of planning and reporting systems the entity will use).
- Evaluating control deficiencies and the impact on the ongoing and long-term effectiveness of the system of internal control (e.g., meeting regularly with senior management from each of the operating units such as, research and development, production, marketing, sales) and major business-enabling functions such as finance, human resources, legal, compliance, risk management to evaluate how they are carrying out their internal control responsibilities.

497 In certain jurisdictions, the CEO (and in some cases also the chief financial officer) is required by law to specifically certify the effectiveness of internal control over financial reporting.

Chief Financial Officer

498 The chief financial officer (CFO) supports the CEO in front-line responsibilities, including internal control over financial reporting. The CFO is integrally involved when the entity's strategies are decided, objectives are specified, risks are analyzed, and decisions are made on how changes will be managed.

499 The CFO provides valuable input and direction and is positioned to focus on evaluating and following up on the actions decided by management. As such, the CFO is an equal partner with the other functional heads. Narrowing this role (e.g., limiting it to financial reporting and treasury) can limit the entity's ability to succeed.

500 In certain jurisdictions, the CFO is required by law to certify to the effectiveness of internal control over financial reporting, alongside the CEO.

Other Members of Senior Management

501 Senior management comprises not only the CEO and CFO but also the other senior executives leading the key operating units and business-enabling functions. Examples include:

- Chief administrative officer
- Chief audit executive and, depending on the size of the entity, chief compliance officer
- Chief information officer
- Chief operating officer
- Chief risk officer
- Other senior leadership roles, depending on the nature of the business

502 Senior management guides the development and implementation of internal control policies and procedures that address the objectives of their functional or operating unit and verify that they are consistent with the entity-wide objectives. They provide direction, for example, on a unit's organizational structure and personnel hiring and training practices, as well as budgeting and other information systems that promote control over the unit's activities. As such, through a cascading responsibility structure, each executive is a CEO for his or her sphere of responsibility.

503 Senior management assigns responsibility for establishing even more specific internal control procedures to those personnel responsible for the unit's functions or departments. These subunit managers can play a more hands-on role in devising and executing particular internal control procedures. Often, these managers are directly responsible for determining resource requirements, training needs, and internal control procedures that address unit objectives, such as developing authorization procedures for purchasing raw materials, accepting new customers, or reviewing production reports to monitor product output. They also make recommendations on the controls, monitor their application within processes, and meet with upper-level managers to report on the operation of controls.

504 Depending how many layers of management exist, these subunit managers, or lower-level supervisory personnel, are directly involved in executing policies and procedures at a detailed level. It is their responsibility to execute remedial actions as control exceptions or other issues arise. This may involve investigating data-entry errors, transactions flagged on exception reports, departmental expense budget variances, or customer back orders or product inventory positions. Issues are communicated up the organization's reporting structure according to the level of severity. Issues requiring senior management oversight include financial performance, product quality, product safety, workplace safety, community involvement, compliance with emission targets, or other areas related to the achievement of the entity's objectives.

505 Management's responsibilities come with specific authority and accountability. Each manager is accountable to the next higher level for his or her portion of the internal control system, with the CEO being ultimately accountable to the board of directors, and the board being accountable to shareholders or other owners of the entity.

Business-Enabling Functions

506 Various organizational functions or operating units support the entity through specialized skills, such as risk management, finance, controllers, product/service quality management, technology, compliance, legal, human resources, and others. They provide guidance and assessment of internal control related to their areas of expertise, and it is incumbent on them to share and evaluate issues and trends that transcend organizational units or functions. They keep the organization informed of relevant requirements as they evolve over time (e.g., new or changing laws and regulations across a multitude of jurisdictions). Such business-enabling functions are referred to as the second line of defense, while front-line personnel execute their control activities.

507 While all controls function to serve a purpose, their efforts are coordinated and integrated as appropriate. For example, a company's new customer acceptance process may be reviewed by the compliance function from a regulatory perspective, by the risk management function from a concentration risk perspective, and by the internal audit function to assess the design and effectiveness of controls. Disruptions to the business process are minimized when the timing and approach to reviews and management of issues are coordinated to the extent possible. Integration of efforts helps create a common language and platform for evaluating and addressing internal control matters, as business-enabling functions guide the organization in achieving its objectives.

Risk and Control Personnel

508 Risk and control functions are part of the second line of defense. Depending on the size and complexity of the organization, dedicated risk and control personnel may support functional management to manage different risk types (e.g., operational, financial, quantitative, qualitative) by providing specialized skills and guidance to front-line management and other personnel and evaluating internal control. These activities can be part of an entity's centralized or corporate organization or they can be set up with "dotted line" reporting to functional heads. Risk and control functions are central to the way management maintains control over business activities.

509 Responsibilities of risk and control personnel include identifying known and emerging risks, helping management develop processes to manage such relevant risks, communicating and providing education on these processes across the organization, and evaluating and reporting on the effectiveness of such processes. The chief risk/control officer is responsible for reporting to senior management and the board on significant risks to the business and whether these risks are managed within the entity's established tolerance levels, with adequate internal control in place. Despite such significant responsibilities, risk and control personnel are not responsible for executing controls, but support overall the achievement of internal control.

Legal and Compliance Personnel

510 Counsel from legal professionals is key to defining effective controls for compliance with regulations and managing the possibility of lawsuits. In large and complex organizations, specialized compliance professionals can be helpful in defining and assessing controls for adherence to both external and internal requirements. The chief legal/compliance officer is responsible for ensuring that legal, regulatory, and other requirements are understood and communicated to those responsible for effecting compliance.

511 A close working relationship between business management and legal and compliance personnel provides a strong basis for designing, implementing, and conducting internal control to manage adverse outcomes such as regulatory sanctions, legal liability, and failure to adhere to internal compliance policies and procedures. At smaller organizations, legal and compliance roles may be shared by the same professional, or one of these roles can be outsourced with close oversight by management.

Other Personnel

512 Internal control is the responsibility of everyone in an entity and therefore constitutes an explicit or implicit part of everyone's job description. Front-line personnel constitute the first line of defense in the performance of internal control responsibilities. Examples include:

- *Control Environment*—Reading, understanding, and applying the standards of conduct of the organization
- *Risk Assessment*—Identifying and evaluating risks to the achievement of objectives and understanding established risk tolerances relating to their areas of responsibility
- *Control Activities*—Performing reconciliations, following up on exception reports, performing physical inspections, and investigating reasons for cost variances or other performance indicators
- *Information and Communication*—Producing and sharing information used in the internal control system (e.g., inventory records, work-in-process data, sales or expense reports) or taking other actions needed to effect control
- *Monitoring Activities*—Supporting efforts to identify and communicate to higher-level management issues in operations, non-compliance with the code of conduct, or other violations of policy or illegal actions

513 The care with which those activities are performed directly affects the effectiveness of the internal control system. Internal control relies on checks and balances, including segregation of duties, and on employees not "looking the other way." Personnel understands the need to resist pressure from superiors to participate in improper activities, and channels outside normal reporting lines are available to permit reporting of such circumstances.

Internal Auditors

514 As the third line of defense, internal auditors provide assurance and advisory support to management on internal control. Depending on the jurisdiction, size of the entity, and nature of the business, this function may be required or optional, internal or outsourced, large or small. In all cases, internal audit activities are expected to be carried out by competent and professional resources aligned to the risks relevant to the entity.

515 The internal audit activity includes evaluating the adequacy and effectiveness of controls in responding to risks within the organization's oversight, operations, and information systems regarding. For example:

- Reliability and integrity of financial and operational information
- Effectiveness and efficiency of operations and programs
- Safeguarding of assets
- Compliance with laws, regulations, policies, procedures, and contracts

516 All activities within an organization are potentially within the scope of the internal auditor's responsibility. In some entities, the internal audit function is heavily involved with controls over operations. For example, internal auditors may periodically monitor production quality, test the timeliness of shipments to customers, or evaluate the efficiency of the plant layout. In other entities, the internal audit function may focus primarily on compliance or financial reporting–related activities. In all cases, they demonstrate the necessary knowledge of the business and independence to provide a meaningful evaluation of internal control.

517 The scope of internal auditing is typically expected to include oversight, risk management, and internal control, and assisting the organization in maintaining effective control by evaluating their effectiveness and efficiency and by promoting continual improvement. Internal audit communicates findings and interacts directly with management, the audit committee, and/or the board of directors.

518 Internal auditors maintain an impartial view of the activities they audit through their skills and authority within the entity. Internal auditors have functional reporting to the audit committee and/or the board of directors and administrative reporting to the chief executive officer or other members of senior management.

519 Internal auditors are objective when not placed in a position of subordinating their judgment on audit matters to that of others and when protected from other threats to their objectivity. The primary protection against these threats is appropriate internal auditor reporting lines and staff assignments. These assignments are made to avoid potential and actual conflicts of interest and bias. Internal auditors do not assume operating responsibilities, nor are they assigned to audit activities with which they were involved recently in connection with prior operating assignments.

External Parties

520 A number of external parties can contribute to the achievement of the entity's objectives, whether by performing activities as outsourced service providers or by providing data or analysis to functional/operational personnel. In both cases, functional/operational management always retains full responsibility for the internal control.

Outsourced Service Providers

521 Many organizations outsource business functions, delegating their roles and responsibilities for day-to-day management to outside service providers. Administrative, finance, human resources, technology, legal, and even select internal operations can be executed by parties outside the organization, with the objective of obtaining access to enhanced capabilities at a lower cost. For example, a financial institution may outsource

its loan review process to a third party, a technology company may outsource the operation and maintenance of its information technology processing, and a retail company may outsource its internal audit function. While these external parties execute activities for or on behalf of the organization, management cannot abdicate its responsibility to manage the associated risks. It must implement a program to evaluate those activities performed by others on their behalf to assess the effectiveness of the system of internal control over the activities performed by outsourced service providers.

Other Parties Interacting with the Entity

522 Customers, vendors, and others transacting business with the entity are an important source of information used in conducting control activities. For example:

- A customer can inform a company about shipping delays, inferior product quality, or failure to otherwise meet the customer's needs for product or service. Or a customer may be more proactive and work with an entity in developing needed product enhancements.
- A vendor can provide statements or information regarding completed or open shipments and billings, which may be used to identify and correct discrepancies and to reconcile balances.
- A potential supplier can notify senior management of an employee's request for a kickback.
- Experts can provide market data to help the organization adapt its business model and supporting processes and controls to new challenges and opportunities.
- A non-governmental organization or newspaper may publish reports on working or environmental conditions at a supplier or sub-supplier.

523 Such information sharing between management and external parties can be important to the entity in achieving its operations, reporting, and compliance objectives. The entity has mechanisms in place with which to receive such information and to take appropriate action on a timely basis—that is, it not only addresses the particular situation reported, but also investigates the underlying source of an issue and fixes it.

524 In addition to customers and vendors, other parties, such as creditors, can provide insight on the achievement of an entity's objectives. A bank, for example, may request reports on an entity's compliance with certain debt covenants and recommend performance indicators or other desired targets or controls.

Independent Auditors

525 In some jurisdictions, the auditor is engaged to audit or examine the effectiveness of internal control over external financial reporting in addition to auditing the financial statements. Based on the audit, the auditor is often able to provide information to management that will be useful in conducting its oversight responsibilities, in particular by communicating:

- Audit findings, analytical information, and recommendations for use in taking actions necessary to achieve established objectives

- Findings regarding deficiencies in internal control that come to its attention, and by making recommendations for improvement

526 In some jurisdictions, the auditor is also legally required to express an opinion on the effectiveness of the internal control over external financial reporting in addition to his or her opinion on the financial statements. Notwithstanding the depth and nature of the independent auditor's work, this is not a replacement or a supplement to an adequate system of internal control, which remains the full responsibility of management.

527 Such information frequently relates not only to financial reporting but to operations and compliance activities as well. The information is reported to and acted upon by management and, depending on its significance, to the board of directors or audit committee.

External Reviewers

528 Subject matter specialists can be solicited or mandated to review specific areas of the organization's internal control. Recognizing the various requirements or expectations of its stakeholders, an organization often seeks expert advice to translate these into policies and procedures, as well as communications and training, and evaluation of adherence to such requirements and standards. Workplace safety, environmental concerns, and fair trade practices are some examples of areas where an organization proactively seeks to ensure that it is complying with governing rules and standards. Certain functional areas may also be reviewed to promote greater effectiveness and efficiency of operations, such as compliance reviews, information systems penetration testing, and employment practices assessments.

Legislators and Regulators

529 Legislators and regulators can affect the internal control systems through specific requirements to establish internal control across the organization and/or through examinations of particular operating units. Many entities have long been subject to legal requirements for internal control. For example, companies listed on a US stock exchange are expected to establish and maintain a system of internal control, and legislation requires that senior executives of publicly listed companies certify to the effectiveness of their company's internal control over financial reporting.

530 Various regulations require that public companies establish and maintain internal accounting control systems that satisfy specified objectives. Various laws and regulations apply to financial assistance programs, which address a variety of activities ranging from civil rights to cash management, and specify required internal control procedures or practices. Several regulatory agencies directly examine entities for which they have oversight responsibility. For example, federal and state bank examiners conduct examinations of banks and often focus on certain aspects of the banks' internal control systems. These agencies make recommendations and are frequently empowered to take enforcement action. Thus, legislators and regulators affect the internal control systems in several ways:

- They establish rules that provide the impetus for management to establish an internal control system that meets statutory and regulatory requirements.

- Through examination of a particular entity, they provide information used by the entity's internal control system and provide comment letters, recommendations, and sometimes directives to management on needed internal control system improvements.
- They may receive and, in turn, investigate, whistle-blower allegations.

Financial Analysts, Bond Rating Agencies, and the News Media

531 Financial analysts, rating agencies, and news media personnel analyze management's performance against strategies and objectives by considering historical financial statements and prospective financial information, actions taken in response to conditions in the economy and marketplace, potential for success in the short and long term, and industry performance and peer-group comparisons, among other factors. Such investigative activities can provide insights, among many other outcomes, into the state of internal control and how management is responding to enhancing internal control.

C. Specific Considerations for Smaller Entities

Characteristics of Smaller Entities

532 Many different perceptions exist as to what constitutes a "smaller" entity. Some think of a local, family-owned hardware store or corner bakery as a typical small business. Others may think of a not-for-profit entity that generates several million dollars in annual donations. Still others see a small entity in the context of a company that has been public for many years manufacturing an innovative product, and which now generates annual revenue of several hundred million dollars with hopes that future growth will catapult it to the Fortune 500 category. Depending on perspective, any or all of these may be considered "smaller" entities.

533 The Framework does not provide a definition in terms of revenue, capitalization, or other factors; that is the role of regulators or other parties. Instead, the term "smaller" rather than "small," suggesting there is a wide range of entities to which these considerations apply. The focus here is on smaller entities that have many of the following characteristics:

- Fewer lines of business and fewer products within lines
- Concentration of marketing focus by channel or geography
- Leadership by management with significant ownership interest or rights
- Fewer levels of management with wider spans of control
- Less complex transaction processing systems
- Fewer personnel, many having a wider range of duties
- Limited ability to maintain deep resources in line as well as support staff positions such as legal, human resources, accounting, and internal auditing

534 The last bulleted item, limited ability to maintain deep resources, is a frequent cause of smaller entities being lower on the economies-of-scale curve. Often, but not always, smaller entities have a higher per-unit cost of producing a product or providing a service. On the other hand, many smaller entities achieve competitive advantage in cost savings through innovation, lower overhead (by retaining fewer people and substituting variable for fixed costs via a part-time workforce or variable compensation plans), and a narrower focus in terms of product, location, and complexity.

535 Economies of scale is often a factor affecting support functions, including those directly relevant to internal control. For example, establishing an internal audit function within a hundred-million-dollar entity likely would require a larger percentage of economic resources than would be the case for a multi-billion-dollar entity. Certainly, the smaller entity's internal audit function would be smaller, and might rely on co-sourcing or outsourcing to provide needed skills, where the larger entity's function might have a broad range of experienced personnel in-house. But in all likelihood the relative cost for the smaller entity would be higher than for the larger one.

536 None of the above characteristics by themselves are definitive. Certainly, size, by whatever measure—revenue, spending, personnel, assets, or other—affects and is affected by these characteristics, and shapes our thinking about what constitutes "smaller."

Meeting Challenges in Attaining Cost-Effective Internal Control

537 The characteristics of smaller entities tend to provide significant challenges for cost-effective internal control. Often managers of smaller entities view control as an administrative burden to be added to existing business processes, rather than recognizing the business need for and benefit of effective internal control that is integrated with core processes.

538 Among the challenges are:

- Obtaining sufficient resources to achieve adequate segregation of duties
- Balancing management's ability to dominate activities, with significant opportunities for improper management override of processes in order to appear that business performance goals have been met
- Recruiting individuals with requisite expertise to serve effectively on the board of directors and committees
- Recruiting and retaining personnel with sufficient experience and skill in operations, reporting, compliance, and other disciplines
- Taking critical management attention from running the business in order to provide sufficient focus on internal control
- Controlling information technology and maintaining appropriate general and application controls over computer information systems with limited technical resources.

539 Despite resource constraints, smaller entities usually can meet these challenges and succeed in attaining effective internal control in a reasonably cost-effective manner.

Segregation of Duties

540 Many smaller entities have limited numbers of employees performing various functions, which sometimes results in inadequate segregation of duties. There are, however, actions that management can take to compensate for this circumstance. Following are some types of controls that can be implemented:

- *Review Reports of Detailed Transactions*—Managers review on a regular and timely basis system reports of the detailed transactions.
- *Review Selected Transactions*—Managers select transactions for review of supporting documents.
- *Take Periodic Asset Counts*—Managers periodically conduct counts of physical inventory, equipment, or other assets and compare them with the accounting records.

- *Check Reconciliations*—Managers from time to time review reconciliations of account balances such as cash or perform them independently.

541 Segregation of duties is not an end in itself, but rather a means of mitigating a risk inherent in processing. When developing or assessing controls that address risks in an entity with limited ability to segregate duties, management should consider whether other controls satisfactorily address these risks and are applied conscientiously enough to reduce risk.

Management Override

542 Many smaller entities are dominated by the founder or other strong leader who exercises a great deal of discretion and provides personal direction to other personnel. This positioning may be key to enabling the entity to meet its growth and other objectives, and can also contribute significantly to effective internal control. With this leader's in-depth knowledge of different facets of the enterprise—its operations, processes, array of contractual commitments, and business risks—he or she is positioned to know what to expect in reports generated by the system and to follow up as needed. Such concentration of knowledge and authority, however, comes with a downside: the leader typically is able to override established procedures.

543 There are a few basic but important things that can help to mitigate the risk of management override.

- Maintain a corporate culture where integrity and ethical values are held in high esteem, embedded throughout the organization, and practiced on an everyday basis. This can be supported and reinforced by recruiting, compensating, and promoting individuals where these values are appropriately reflected in behavior.
- Implement a whistle-blower program, where personnel feel comfortable reporting any improprieties, regardless of the level at which they may be committed. Importantly, there must be ability to maintain anonymity and confidence that reported matters will be investigated thoroughly and acted upon, appropriately and without reprisals. It usually is important that where circumstances warrant matters can be reported directly to the board or audit committee.
- Position an effective internal audit function to detect instances of wrongdoing and breakdowns at the entity and sub-unit levels. Ready access to relevant information and ability to communicate directly with and senior management and the board or audit committee are key factors.
- Attract and retain qualified board members that take their responsibilities seriously to perform the critical role of preventing or detecting instances of management override.

544 Such practices mitigate the risk of impropriety and promote accountability of leadership, while gaining the unique advantages of cost-effective internal control in a smaller entity environment.

Board of Directors

545 The discussion above highlights the need for a board of directors with requisite expertise to perform its oversight responsibilities well. With appropriate knowledge, attention, and communication, the board is positioned to provide an effective means of offsetting the effects of improper management override. In smaller entities, board directors typically have in-depth knowledge of what usually are relatively straightforward business operations, and they communicate more closely with a broader range of personnel. Many smaller entities, however, find it very difficult to attract independent directors with the desired skills and experience. Typical challenges to finding suitable directors include inadequate knowledge of the entity and its people, the entity's limited ability to provide compensation commensurate with board responsibilities, a sense that the chief executive might be unaccustomed or unwilling to appropriately share governance responsibilities, or concerns about potential personal liability.

546 Some entities have been willing to address the concerns of desired board candidates and have expanded their search to broader populations with financial and accounting and other valued expertise. In this way, they can shape the the board to not only appropriately monitor senior management, but also to provide value-added advice.

Information Technology

547 Many smaller entities do not have the extensive technical resources necessary to develop, maintain, and operate software in an adequately controlled manner. Thus, these entities consider alternatives to meet their information and control needs.

548 Many smaller entities use software developed and maintained by others. These packages still require controlled implementation and operation, but many of the risks associated with systems developed in-house are reduced. For example, typically there is less need for program change controls, inasmuch as changes are done exclusively by the developer, and generally the personnel in a smaller entity don't have the technical expertise to attempt to make unauthorized program modifications.

549 Commercially developed packages can bring additional advantages. Such packages may provide embedded facility for controlling which employees in the entity can access or modify specified data, performing checks on data processing completeness and accuracy, and maintaining related documentation.

Monitoring Activities

550 The monitoring activities component is an important part of the Framework, where a wide range of activities routinely performed by managers in running a business can provide information on the functioning of other components of the internal control system. Management of many smaller entities regularly perform such activities, but have not always taken sufficient credit for their contribution to the effectiveness of internal control. These activities, usually performed manually and sometimes supported by computer software, should be fully considered in designing, implementing, and conducting internal control and assessing the effectiveness of internal control.

D. Methodology for Revising the Framework

Background

551 In November 2010, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) announced a project to review and update its Internal Control—Integrated Framework (Framework). This initiative was expected to make the existing Framework and related evaluation tools more relevant in the increasingly complex industry, operating and regulatory environment so that organizations worldwide could better design, implement, and conduct internal control and assess its effectiveness. As the original author of the Framework, PwC conducted this project by bringing together in-depth understanding of the 1992 Framework and rationale for decisions made in creating the Framework, and sought input from users, stakeholders, and senior resources who provided current perspectives on internal control.

552 The Framework has been widely accepted by organizations in implementing, designing, conducting , and assessing internal control relating to operations, compliance, and financial reporting objectives, and more recently to internal control over financial reporting in compliance with the US Sarbanes-Oxley Act of 2002 (SOX) and similar regulatory requirements in other countries. Enhancement provided by this project is not intended to change how internal control is defined, assessed, or managed, but rather to provide relevant conceptual guidance and practical examples.

Project Structure

553 The COSO Board formed an Advisory Council comprising representatives from industries, academia, government agencies, and non-profit entities, and observers from regulators and standard setters to provide input as the project progressed. In addition, the Framework has been exposed to the public to capture additional input. Such due process has helped the update adequately address current challenges for organizations within their internal control.

Approach

554 The project consisted of four phases:

- *Assess and Envision*—Through literature reviews, global surveys, and public forums, this phase identified current challenges for organizations in implementing the Framework. During this phase, the PwC Project Team analyzed information, reviewed various sources of input, and identified critical issues and concerns. COSO launched a global survey, available to the general public for providing input on the Framework, soliciting over 700 responses.
- *Build and Design*—The PwC ProjectTeam developed the update, including principles and points of focus. The update draft was reviewed by key users and stakeholder groups to solidify reactions and suggestions.
- *Preparation for Public Exposure*—The PwC Project Team refined the update through reviews with the general public. The COSO Board and Advisory Council also considered whether the updated Framework was sound, logical, and useful to management of all sizes.
- *Public Exposure*—In this phase, the Framework was issued for public exposure for a 104-day comment period. Once the comments were received. The PwC Project Team reviewed and analyzed them, and identified any needed modifications. The updated Framework is also made available for comment during the public exposure of the companion documents: *Internal Control over External Financial Reporting*: *Compendium of Approaches and Examples*, and *Illustrative Tools for Assessing Effectiveness of a System of Internal Control*.
- *Finalization*—The PwC Project Team will finalize the Framework and related publications and provide these documents to the COSO Board for review and acceptance.

555 Within each project phase and between phases, as one might expect, many different and sometimes contradictory observations or recommendations were expressed on fundamental issues relating to internal control. The project team, with COSO Board oversight, carefully considered merits of positions put forth, both individually and in the context of related issues, and revised the Framework when they that helped the development of a relevant, logical, and internally consistent publication on internal control.

E. Public Comment Letters

556 As noted in Appendix D, Methodology for Revising the Framework, a draft of the Framework was issued for public comment from December 19, 2011, through March 31, 2012. There were more than 100 public responses to the online survey and 96 public comment letters relating to this exposure draft. These letters contained more than 1,000 comments on many different aspects of the updated Framework, and each comment was considered in further revisions. This appendix summarizes the more significant comments and any resulting modifications to the Framework.

557 Many respondents concurred with COSO that the updates to the Framework are expected to help management strengthen existing systems of internal control by responding to many changes in the business and operating environments over the past twenty years, codifying principles associated with the five components of internal control, and expanding the reporting objective to include other important forms of reporting. There were divergent views as to whether the updates to the Framework would set a higher threshold for attaining effective internal control, impose additional burdens on entities that report on internal control, and should incorporate additional aspects of enterprise risk management.

558 Whereas some respondents sought fundamental changes to the Framework, others recognized that the Framework remains relevant and useful today and should be used as the basis for an update in selected areas, as discussed below.

Definition of Internal Control

559 Some respondents suggested amending the definition in different ways. Individual suggestions included aligning the definition with other standards, embedding risk, removing objective categories, increasing emphasis on the board, adding anti-fraud/ethical behavior expectations, removing the concept of reasonable assurance, expanding the reporting objective to include other aspects such as timeliness and transparency, and stipulating that effectiveness of internal control is attained by reducing the risk of not achieving an objective to an acceptably ***low*** level (emphasis added). Other respondents, however, noted that the original definition has gained wide acceptance (e.g., auditing standards, legislation and guidance) and should be retained.

560 The Framework revises the definition to remove the modifiers from each category of objectives. The reasons for this change are that the objectives are discussed in some detail later in Chapter1 "Definition of Internal Control", and with the broadening of the reporting category, respondents appropriately identified additional relevant aspects of the reporting objective beyond just reliability.

561 Other than this change, the Framework retains a broad definition as other suggestions are either encompassed in the definition, as amended, or are discussed more appropriately as part of the components of internal control. Finally, incorporating the notion of reducing risk to a low level potentially pre-empts management's judgment as being too restrictive for some objectives.

Reporting, Operations, and Compliance Objectives

562 Some respondents called for reconsidering the expansion of financial reporting objectives and potential regulatory implications, and reconsidering the measurability of the achievement of operations objectives.

563 The Framework retains descriptions of the three categories of objectives, provides supplemental descriptions of operations and compliance objectives, and clarifies that an operations objective can be achieved when a suitable external standard exists.

Principles

564 Respondents acknowledged the benefit of codifying into principles internal control concepts introduced in the original framework and that these principles provide clarity for management in designing, implementing, and conducting internal control, and assessing the effectiveness of systems of internal control.

565 Some respondents suggested folding Principle 11, Selects and Develops General Controls over Technology, into Principle 10, Selects and Develops Control Activities, based on a view that selecting and developing technology general controls is a subset of selecting control activities in general, which are part of Principle 10.

566 Some also suggested combining Principle 8, Assessing Fraud Risk, into Principle 7, Identifies and Analyzes Risks, on the basis that fraud risk may be viewed as only one type of risk potentially impacting objectives.

567 The Framework carries forward the seventeen principles. It retains the principles that focus on the use of technology and the assessment of fraud risks, recognizing their important role in achieving effective internal control. Some principles were also enhanced or clarified based on respondents' comments.

Assessing Effectiveness

Attributes

568 Some respondents expressed concern that including attributes (renamed as points of focus) may trigger an undesirable checklist mentality by management, auditors, and regulators. Other respondents requested clarity on whether attributes represent requirements relating to whether principles are present and functioning or whether the Framework presumes that attributes are present and functioning.

569 The Framework now replaces the term "attributes" with "points of focus," consistent with the original framework, to reduce the perception that the use of points of focus is a requirement. The Framework clarifies the relevance of points of focus by positioning them as important considerations in determining whether a principle is present and functioning as part of a component, allowing management greater flexibility to exercise judgment in considering which points of focus are relevant for the entity. Management may use the points of focus presented in the Framework and/or other considerations

depending on the entity's industry, operations, and regulatory environment. Accordingly, the Framework was revised to remove the presumption that points of focus must be present and functioning.

570 Points of focus have been removed from Chapter 3, Effective Internal Control, to clarify that they are not to be considered requirements associated with the relevant principles. Instead, they are introduced and their relevance clarified in Chapter 4, Additional Considerations. Within the respective component chapters, they are listed after the principle to which they apply.

Classification of Internal Control Deficiencies

571 Some respondents suggested removing major and minor non-conformities, and using a consistent terminology for all categories of objectives in the Framework. Some further suggested using terms "significant deficiency" and "material weakness" for all categories.

572 The Framework presents a revised terminology when generally referring to the severity of deficiencies, and uses the terms "deficiencies" and "major deficiencies." However, the Framework acknowledges that the terms "significant deficiency" and "material weakness" are used in the context of external laws, standards, and regulations, and that the user will need to consider specific terms and criteria established by such laws, standards, and regulations.

Objective-Setting

573 Some respondents suggested that the Framework include objective-setting as a component of internal control. Others suggested that objective-setting remain a precondition of internal control, and that the Framework provide greater clarity of the role of assessing suitability of objectives within internal control.

574 The Framework retains the five components and the concept that establishing objectives is a precondition to internal control. It clarifies the distinction between establishing objectives (outside the system of internal control) and specifying objectives (within the system of internal control) in Chapter 2, Objectives, Components, and Principles. The Framework expands discussion on suitability of objectives and explains how management should respond when specified objectives are viewed as unsuitable within the Risk Assessment chapter.

Objectives

Safeguarding of Assets

575 Some respondents suggested including safeguarding of assets as a category of objectives based on established laws, regulations, and standards. Others suggested that safeguarding of assets is part of each category of objectives.

576 The Framework retains safeguarding of assets as an operations objective, consistent with the original framework. The *Internal Control-Integrated Framework, Addendum to Reporting Parties* (May 1994) affirmed that the definition of internal control relates to operations, compliance, and financial reporting objectives, as set out in the original framework, and remains appropriate. The *Addendum* also concluded that when management reports on internal control over financial reporting there is a reasonable expectation that such report covers controls to help prepare financial statements and prevent or detect in a timely manner any unauthorized acquisition, use, or disposition of assets.

577 The Framework acknowledges that some laws, regulations, and standards have established safeguarding of assets as a separate category of objective. When management reports on an entity's system of internal control, there may be established objectives or sub-objectives relating to physical security, prevention, or timely detection of unauthorized acquisition, use, or disposition of assets. The Framework retains the view that safeguarding of assets is primarily related to operations, but may be viewed within the context of reporting and compliance objective categories.

Strategic Objectives

578 Some respondents suggested the addition of strategic objectives as a category of objectives. Some also suggested that this change was already made in *Enterprise Risk Management–Integrated Framework* and that the Framework should adopt a similar change.

579 The Framework retains operations, reporting, and compliance objective categories and the concept that strategic objectives are not part of internal control. Including strategy-setting and strategic objectives would require adding other concepts, including risk appetite and risk tolerance, to provide a complete discussion of this objective category. These concepts are more appropriate in the context of enterprise risk management, as discussed below.

Enterprise Risk Management

580 Some respondents called for further integration of enterprise risk management concepts into internal control, in particular seeking an expanded discussion of risk tolerance and adding risk appetite. Some also sought a merger of COSO's *Enterprise Risk Management—Integrated Framework* (*ERM Framework*) with the Framework. Others supported keeping the two frameworks separate and distinct.

581 The COSO Board considered merging the two frameworks and decided to keep them separate and distinct. Accordingly, strategy-setting, strategic objectives, and risk appetite remain part of the *ERM Framework*. The Framework retains the definition of risk appetite and the application of risk tolerance and retains strategy-setting as a precondition of internal control.

582 The Framework expands the Foreword to acknowledge that the two frameworks are intended to be complementary, neither superseding the other. The Framework includes a discussion of overlapping concepts in Appendix G.

Smaller Entities and Governments

583 Some respondents called for expanded guidance specific to smaller entities and governments. Some suggested that the Framework specifically highlight the differences in applicability to such entities. Others suggested that the length of document is potentially overwhelming for smaller organizations.

584 The Framework contains additional discussion relating to Principle 2, Exercises Oversight Responsibility concerning smaller entities. Additional discussion from the 2006 COSO *Guidance for Smaller Public Entities* is included in Appendix C. This appendix has been expanded to consider entities beyond smaller public companies and has relevance for other smaller entities.

Technology

585 Some respondents commented, in general, on expanding the guidance on technology in the Framework. Others suggested including detailed technology topics such as backup and recovery in Principle 11, Selects and Develops General Controls over Technology. And still others suggested adding detailed risks associated with current technology initiatives such as cloud computing or continuous auditing techniques. Some recommended referring to or incorporating other established frameworks specifically addressing technology controls and other considerations.

586 The Framework includes enhanced discussion on technology both in the points of focus and in various chapters. The Framework does not include extensive discussion on specific current technology initiatives or the risks associated with them because of the evolving nature of technology and concerns that the Framework may become dated. The Framework does not explicitly reference other technology-focused frameworks by name.

Structure and Layout

587 Some respondents expressed concern about the length of the Framework and suggested presenting only those requirements of internal control. Others suggested revising the structure to emphasize requirements versus supplemental guidance.

588 The COSO Board continues to believe that the Framework comprises all chapters. The Board acknowledges, however, the importance of clearly setting forth that components and relevant principles are requirements of an effective system of internal control.

F. Summary of Changes to the Internal Control—Integrated Framework Issued in 1992

589 This Appendix summarizes the broad changes from the original edition issued in 1992, as well as changes made within each of the five components of internal control.

Broadbased Changes

590 The following significant changes are evident across all areas of the Framework:

- *Applies a principles-based approach*—The updated Framework focuses greater attention on principles. While the original framework implicitly reflected the core principles of internal control, the 2012 version explicitly states the seventeen principles, which represent the fundamental concepts associated with the components of internal control. These principles remain broad as they are intended to apply to for-profit companies, including publicly traded and privately held companies; not-for-profit entities; government bodies; and other organizations. Supporting each principle are points of focus, representing characteristics associated with the principles. The components and principles comprise the criteria that will assist management in assessing whether an entity has effective internal control.
- *Expands the reporting category of objectives*—The financial reporting objective category is expanded to consider other external reporting beyond financial reporting, as well as internal reporting, both financial and non-financial.
- *Clarifies the role of objective-setting in internal control*—The original framework stated that objective-setting was a management process, and that establishing objectives is a pre-condition to internal control. The updated Framework preserves that view and expands the discussion on specifying objectives and considered suitability of established objective. This discussion is included in Chapter 2, Objectives, Components, and Principles.
- *Enhances governance concepts*—The updated publication includes expanded discussion on governance relating to the board of directors and committees of the board, including audit, compensation, nomination/governance committees.
- *Considers globalization of markets and operations*—Organizations expand beyond domestic markets in the pursuit of value, entering into international markets, and executing cross-border mergers and acquisitions. The updated Framework discusses changes in management operating models, legal entity structures, and related roles, responsibilities and accountabilities for internal control at the entity and subunits level. In addition, it considers the identification and analysis of internal and external risk factors relating to mergers and acquisitions.

- *Considers different business models and organizational structures*—Business models and structures have evolved over the past twenty years, and many entities now expand their business models to encompass the use of outsourced service providers to provide products or services necessary to the ongoing operation of the entity. The competitive landscape, globalization, dynamic industry and technological changes, evolving business models, competition for talent, cost management, and other factors have required management to look beyond internal operations to access needed resources. The updated Framework explicitly considers the extended business model, including the responsibilities for internal control in this model and the achievement of effective internal control.
- *Considers demands and complexities in laws, rules, regulations, and standards*—Regulators and standard setters promote greater stakeholder protection and confidence in external reporting through changes in laws, rules, regulations, and standards. The updated Framework recognizes the roles of regulators and standard-setters in establishing objectives and in providing criteria to assess the severity and to report internal control deficiencies.
- *Considers expectations for competencies and accountabilities*—Demands for greater competence and accountability increase as organizations grow more complex, acquire entities, restructure, introduce new products and services, and implement new processes and technologies. Organizations may flatten and shift management operating models and delegate greater authority or accountability. The updated Framework broadens the discussion on these topics.
- *Reflects the increased relevance of technology*—The number of entities that use or rely on technology has grown substantially since 1992, along with the extent that technology is used in most entities. Technologies have evolved from large standalone mainframe environments that process batches of transactions to highly sophisticated, decentralized, and mobile applications involving multiple real-time activities that can cut across many systems, organizations, processes, and technologies. The change in technology can impact how all components of internal control are implemented.
- *Enhances consideration of anti-fraud expectations*—The original framework considered fraud, although the discussion of anti-fraud expectations and the relationship between fraud and internal control was less prominent. This 2012 Framework contains considerably more discussion on fraud and also considers the potential of fraud as a principle of internal control.

Overall Framework Layout

591 The original framework contained one chapter that presented the definition of internal control, the components of internal control, the relationship of objectives and components, and effectiveness. In the revised Framework, these topics are covered in three different chapters: Chapter 1, Definition of Internal Control defines internal control; Chapter 2, Objectives, Components and Principles, discusses components of internal control and the relationship of objectives, components, and principles; and Chapter 3,

592 Effective Internal Control, considers the requirements for assessing the effectiveness of a system of internal control. Further, Chapter 4, Additional Considerations, discusses management judgment, points of focus, cost versus benefits of internal control, the changing role of technology, documentation, and application of internal control in larger versus smaller entities.

Key Changes to Internal Control Components

Control Environment

593 In the two decades since the publication of the original framework in 1992, a number of factors have pointed to the need for an update on what to consider in establishing a sound control environment. There is now greater complexity in business models, with enterprises extending to a wide network of third parties and business partners that are not only accountable for delivering results but also for adhering to expected standards that the organization seeks to uphold. The multiple structures that define organizations today, whether by product line, geography, legal entity, or some other factor, require a flexible and multidimensional approach to governance and control and the ability to report accordingly.

594 Today, there is an increased need for transparency of how the organization operates and governs itself; reporting now extends beyond financial performance; risk discussions are expected to be more robust and detailed; corporate social responsibility reporting matters more to stakeholders; and the pace for publishing such information has accelerated. Changes in expectations of governance as a result of regulatory developments, listing standards, and other stakeholder requirements have mandated certain structures and processes. These include independence of board members, disclosures of skill profiles, processes for board and audit committee evaluation, and alignment of incentives, pressures, and rewards to ensure the right behavior is promoted and negative behavior is corrected. All of this is designed to keep pace with the evolving risk profile of the organization.

595 In the updated the Control Environment (Chapter 5), key changes include:

- Combining into five principles the discussions relating to integrity and ethical values, commitment to competence, board of directors or audit committee, management's philosophy and operating style, organizational structure, assignment of authority and responsibility, and human resource policies and practices
- Explaining linkages between the various components of internal control to demonstrate the foundational aspects of the control environment for a sound system of internal control (e.g., income statement level)
- Expanding the discussion of governance roles in an organization, recognizing differences in structures, requirements, and challenges across different jurisdictions, sectors, and types of entities

- Clarifying the expectations of integrity and ethical values to reflect lessons learned and developments in ethics and compliance (e.g., codes of conduct, the attestation process, whistle-blower processes, investigation and resolution, and training and reinforcement both internally and with third parties)
- Expanding the notion of risk oversight and strengthening the linkages between risk and performance to help allocate resources to support internal control in the achievement of the entity's objectives
- Emphasizing the need to consider internal control across the complexities in organizational structure resulting from different business models and the use of outsourced service providers, business partners, and other external partners
- Aligning roles and responsibilities discussed in organizational structure with the information presented in Appendix B (Roles and Responsibilities) so that major roles are used consistently within the Framework

Risk Assessment

596 Since 1992, the attention given to on risk and the risk assessment component of internal control has continued to increase, with risk and control being more closely aligned. Consequently, many organizations have shifted their thinking away from being prescriptive to taking a more risk-based approach to internal control. Some users of the original framework suggested that updates were needed to further enhance the understanding of risk and its link to the overall system of internal control. As companies embrace risk management and enterprise risk management programs, they are also seeking greater clarity of how risk assessments are considered in the context of internal control, and what aspects of risk management remain incremental to internal control.

597 Users also noted that almost half of the original chapter on Risk Assessment focused on objectives, and that this focus was not needed if objective-setting was truly a pre-condition to internal control. Many organizations have expanded their reporting efforts, moving to include many other types of external reporting beyond just financial reporting. Finally, often in response to events occurring within their organizations, industry, or within the general business community, and as a result of expanding legislative pressures in some jurisdictions, many organizations have also increased their efforts relating to anti-fraud efforts.

598 Therefore, Chapter 6, Risk Assessment, reflects these key changes:

- Repositioning much of the discussion on objective-setting, which continues to be viewed as a pre-condition to risk assessment, to Chapter 2, Objectives, Components, and Principles, and no longer including the discussion on categories of objectives, linkage between objectives, and achievement of objectives in the Risk Assessment component
- Focusing the Risk Assessment component on articulating objectives relating to operations, reporting, and compliance with sufficient clarity so that any risks to those objectives can be identified and assessed, and considering the need to assess the suitability of objectives for use as a basis for assessing effectiveness

- Broadening the financial reporting category of objectives to include other aspects of external reporting and to include internal reporting
- Reflecting the view that non-financial reporting is conducted in relation to an external requirement or standard
- Clarifying that risk assessment includes processes for risk identification, risk analysis, and risk response
- Expanding the discussion on the risk severity beyond impact and likelihood to include such velocity and persistence
- Incorporating risk tolerances (set as a precondition to internal control and pertaining to the level of acceptable variation in performance and the relative importance of objectives) into the assessment of acceptable risk levels
- Expanding the discussion on management needing to understand significant changes in its internal and external factors and how those might impact the overall system of internal control
- Considering fraud risk relating to material misstatement of reporting, inadequate safeguarding of assets, and corruption as part of the risk assessment process

Control Activities

599 Since 1992, the evolving role of technology in business has perhaps been most evident in the implementation of control activities. While the fundamental concepts around control activities put forth in the original framework have not changed, technology has changed many of the details. Today, information technology is much more integrated into business processes throughout any entity. The variety of technologies being used at most entities has mushroomed beyond largely centralized information systems in an organization's own data center to myriad decentralized, mobile, intelligent and web-enabled technologies, which are increasingly located at third-party service organizations. Also, the recent focus on improving controls in organizations, which has been provoked by the marketplace and regulation, has led to a deeper understanding of how control activities are effectively designed and implemented.

600 Therefore, within Chapter 7, Control Activities, key changes include:

- Broadening the discussion to reflect the evolution in technology since 1992 (e.g., replacing data center concepts with a more general discussion on the technology infrastructure)
- Expanding the discussion of the relationship between automated control activities and general controls over technology to reinforce the linkages to business processes, with the details on automated control activities and general controls over technology separated into discrete sections to clarify the distinction between the two
- Expanding the discussion that control activities constitute a range of control techniques while providing a more detailed description of these types and techniques, and a way to categorize them; making distinct transaction level controls from controls at other levels of the organization; and discussing in more detail information-processing objectives

- Updating the discussion on general technology controls to focus on the more universal concepts of what needs to be controlled in this area rather than specifics applicable to 1992 technology
- Clarifying that control activities are actions established by policies and procedures rather than being the policies and procedures themselves

Information and Communication

601 The source, volume, and form of information and communication have expanded dramatically since 1992. Information sources have grown more diverse and complex, spanning outsourced service providers that support all or part of an organization's business processes (e.g., outsourcing service providers, joint ventures) and internal and external networks designed to create unstructured information-sharing mechanisms (social media).

602 The volume of information, particularly in the form of raw data, accessible to and collected by organizations, creates both opportunity and risk. The scope of regulatory regimes has created greater demand for information, greater expectations for quality and protection, and greater requirements for communication. And, as organizations and business models have become more complex in structure and geographic reach, quality information and its communication within the organization has become an imperative. Additionally, the importance of the free flow of information within the organization to allow management and employees to understand new or changed events or circumstances to re-evaluate risks and modify the internal control system has become more critical as the legal, management, and functional structures of business entities have become more complex.

603 Within Chapter 8, Information and Communication, key changes include:

- Emphasizing the discussion of importance of quality of information
- Expanding the discussion of the expectations for verifying to a source and for retention when information is used to support reporting objectives to external parties
- Expanding the discussion on the impact of regulatory requirements on reliability and protection of information
- Expanding the discussion on the volume and sources of information in light of increased complexity of business processes, greater interaction with external parties, and technology advances
- Reflecting the impact of technology and other communication mechanisms on the speed, means, and quality of the flow of information
- Adding content on the information and communication needs between the entity and third parties, emphasizing the importance of considering how processes may occur outside the entity (e.g., by the use of third-party service providers that manage specific processes) and how the entity needs to obtain information from and communicate with parties that operate outside its legal and operational boundaries

Monitoring Activities

604 In applying the original framework, users often focused monitoring efforts extensively on control activities. With the change in regulatory reporting requirements in many jurisdictions, organizations have begun to consider monitoring in its broader and intended context—assisting management in understanding how all components of internal control are being applied and whether the overall system of internal control operates effectively. To enhance internal consistency among components in the Framework and make the discussion more actionable, the title of this component has been updated to Monitoring Activities and the discussion has been enhanced.

605 The changes to the principles in the Framework will not substantially alter the approaches developed for COSO's Guidance on Monitoring Internal Control Systems.

Within Chapter 9, Monitoring Activities, key changes include:

- Refining the terminology, where the two main categories of monitoring activities are now referred to as "ongoing evaluations" and "separate evaluations"
- Adding the need for a baseline understanding in establishing and evaluating ongoing and separate evaluations
- Expanding discussion of the use of technology and external service providers

G. Comparison with COSO Enterprise Risk Management—Integrated Framework

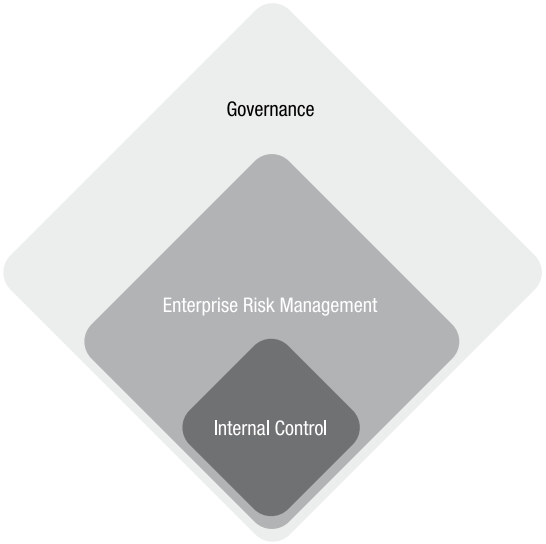
606 In 2004, COSO issued *Enterprise Risk Management—Integrated Framework*, which establishes a framework for enterprise risk management and provides guidance to business and other entities to help them develop and apply their enterprise risk management activities. The Framework identifies and describes eight interrelated components necessary for effective enterprise risk management.

607 The *Enterprise Risk Management—Integrated Framework* defines enterprise risk management as a process, effected by an entity's board of directors, management, and other personnel, applied both in strategy-setting and across the entity, designed to identify potential events that may affect the entity, to manage risk, and to provide reasonable assurance that the objectives of an entity will be achieved.

608 This appendix outlines the relationship between the *Internal Control—Integrated Framework* and the *Enterprise Risk Management—Integrated Framework*.

A Broader Concept

609 Enterprise risk management is broader than internal control, elaborating on internal control and focusing more directly on risk. Internal control is an integral part of enterprise risk management, while enterprise risk management is part of the overall governance process. This relationship is depicted in the illustration below.



610 The publication *Enterprise Risk Management—Integrated Framework* remains in place for entities and others looking broadly at enterprise risk management.

Categories of Objectives

611 Both the *Internal Control—Integrated Framework* and *Enterprise Risk Management—Integrated Framework* cover all reports developed by an entity, disseminated both internally and externally. These include reports used internally by management and those issued to external parties, including regulatory filings and reports to other stakeholders.

612 The two publications handle categories of objectives differently. While both specify the three categories of objectives of operations, reporting, and compliance, *Enterprise Risk Management—Integrated Framework* adds a fourth category: strategic objectives (illustrated in the diagram below). Strategic objectives operate at a higher level than the others. They flow from an entity's mission or vision, and the operations, reporting, and compliance objectives should be aligned with them. Enterprise risk management is applied in setting strategies, as well as in working toward achievement of objectives in the other three categories.

613 An underlying premise of enterprise risk management is that every entity exists to provide value for its stakeholders. Strategic objectives reflect management's choice of how the entity will seek to create value for its stakeholders. Related objectives (referring to operations, reporting, and compliance objectives in the *Enterprise Risk Management—Integrated Framework*) flow from these strategic objectives. While enterprise risk management focuses on how an entity creates, preserves, and realizes value, internal control focuses primarily on the achievement of specified objectives.

614 Enterprise risk management is often viewed as being more forward-looking, considering how much risk the organization is willing to accept, how risks are both created and mitigated from strategic choices, and how emerging risks may impact the organization. In contrast, internal control focuses on whether the organization is mitigating risks to the achievement of specified objectives. In this context, internal control is often more retrospective than prospective.

Risk Appetite and Risk Tolerances

615 The Enterprise Risk Management Framework introduces the concepts of risk appetite and risk tolerance.

- *Risk appetite* is the broad-based amount of risk an entity is willing to accept in pursuit of its mission/vision. It serves as a guidepost in strategy-setting and selecting related objectives.
- *Risk tolerance* is the acceptable level of variation relative to achievement of objectives. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite.

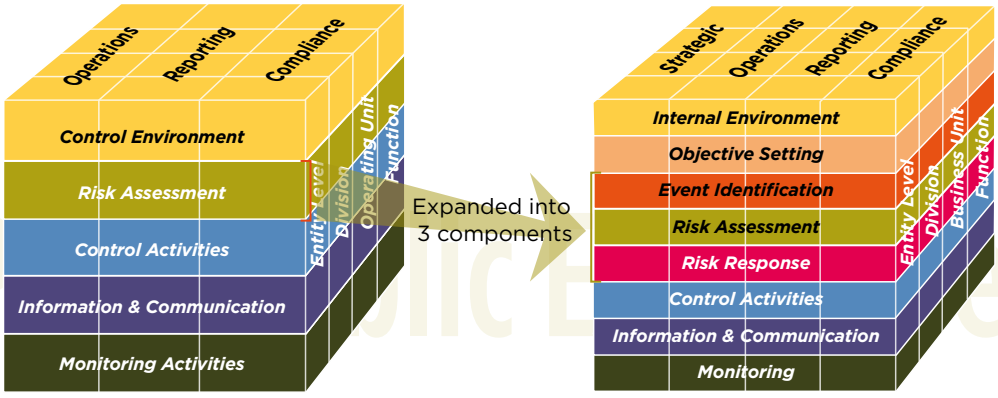
616 Operating within risk tolerance provides management greater assurance that the entity remains within its risk appetite, which in turn provides added comfort that the entity will achieve its objectives. The concept of risk tolerance is included in the Framework, as a pre-condition to internal control, but not as a part of internal control.

Portfolio View

617 Enterprise risk management requires considering composite risks from a portfolio perspective. This concept is not contemplated in the *Internal Control—Integrated Framework*, which focuses on achievement of objectives on an individual basis. Internal control does not require that the entity develop a portfolio view.

Components

618 With the enhanced focus on risk, the *Enterprise Risk Management—Integrated Framework* expands the internal control framework's risk assessment component, creating three components: event identification, risk assessment, and risk response.



Internal Control—Integrated Framework *Enterprise Risk Management—Integrated Framework*

619 The objective-setting component of the *Enterprise Risk Management—Integrated Framework* considers the process used by management and the board for setting operations, reporting, and compliance objectives. Setting risk appetite and risk tolerance are key tenets of enterprise risk management. In contrast, internal control views the setting of objectives and risk tolerance as preconditions to an effective system of internal control.

Summary of Similarities and Differences of Components

620 Each of the five components of internal control are reviewed below in relation to the *Enterprise Risk Management—Integrated Framework*. In each case, a table is included setting out concepts that are:

- Common to both internal control (IC) and enterprise risk management (ERM)
- Included in internal control and expanded upon in enterprise risk management
- Incremental to enterprise risk management and not part of internal control

621 The principles for each component contained in the Framework are used where possible to depict these similarities and differences.

Control Environment

Common to ERM and IC	Introduced in IC and Expanded in ERM	Incremental to ERM
• Demonstrates commitment to integrity and ethical values • Establishes structures, authority, and responsibility • Demonstrates commitment to competence • Enforces accountability	• Exercises oversight responsibility	• Establishes risk management philosophy • Establishes risk culture • Establishes risk appetite

622 In discussing the Control Environment component, the *Enterprise Risk Management—Integrated Framework* discusses (in the chapter titled Internal Environment) an entity's risk management philosophy, which is the set of shared beliefs and attitudes characterizing how an entity considers risks, reflecting its values and influencing its culture and operating style. As described above, the Framework encompasses the concept of an entity's risk appetite, which is supported by more specific risk tolerances.

623 Because of the critical importance of the board of directors and its composition, *Enterprise Risk Management—Integrated Framework* expands on the call for a critical mass of independent directors (normally at least two) stating that for enterprise risk management to be effective, the board must have at least a majority of independent outside directors.

Risk Assessment

Common to ERM and IC	Introduced in IC and Expanded in ERM	Incremental to ERM
• Assesses fraud risk • Identifies and analyzes significant change	• Identifies and analyzes risks/events	• Distinguishes risk and opportunities • Develops portfolio view

624 *Enterprise Risk Management—Integrated Framework* and *Internal Control—Integrated Framework* both acknowledge that risks occur at every level of the entity and result from a variety of internal and external factors. And both frameworks consider risk identification in the context of the potential impact on the achievement of objectives.

625 *Enterprise Risk Management—Integrated Framework* discusses the concept of potential events, defining an event as an incident or occurrence emanating from internal or external sources that affect strategy implementation or achievement of objectives. Potential events with positive impact represent opportunities, while those with negative impact represent risks. Potential events with an adverse impact represent risks. The Framework focuses on identifying risks and does not include the concept of identifying opportunities as the decision to pursue opportunities as part of the broader strategy-setting process.

626 While both frameworks call for assessment of risk, *Enterprise Risk Management—Integrated Framework* suggests viewing risk assessment through a sharper lens. Risks are considered as inherent and residual, preferably expressed in the same unit of measure established for the objectives to which the risks relate. Time horizons should be consistent with an entity's strategies, objectives and, where possible, observable data. *Enterprise Risk Management—Integrated Framework* also calls attention to interrelated risks, describing how a single event may create multiple risks.

627 As noted, enterprise risk management encompasses the need for an entity-level portfolio view, with managers responsible for business unit, function, process, or other activities having a composite assessment of risk for individual units.

628 Like the *Internal Control—Integrated Framework*, the *Enterprise Risk Management—Integrated Framework* identifies four categories of risk response: avoid, reduce, share, and accept. However, enterprise risk management requires additional consideration: potential responses from these categories with the intent of achieving a residual risk level aligned with the entity's risk tolerances. Management also considers as part of enterprise risk management the aggregate effect of its risk responses across the entity and in relation to the entity's risk appetite.

Control Activities

Common to ERM and IC	Introduced in IC and Expanded in ERM	Incremental to ERM
• Selects and develops control activities • Selects and develops general controls over technology • Deploys through policies and procedures		

629 Both frameworks present control activities as helping ensure that management's risk responses are carried out. The *Internal Control—Integrated Framework* presents a more current view of technology and its impact on the running of an entity.

Information and Communication

Common to ERM and IC	Introduced in IC and Expanded in ERM	Incremental to ERM
• Communicates internally • Communicates externally	• Uses relevant information	

630 The *Enterprise Risk Management—Integrated Framework* takes a broader view of information and communication, highlighting data derived from past, present, and potential

future events. Historical data allows the entity to track actual performance against targets, plans, and expectations, and provides insights into how the entity performed in the periods under varying conditions. Current data provides important additional information, and data on potential future events and underlying factors completes the analysis. The information infrastructure sources and captures data in a timeframe and at a depth of detail consistent with the entity's need to identify events and assess and respond to risks and remain within its risk appetite. The *Internal Control—Integrated Framework* focuses more narrowly on data quality and relevant information needed for internal control.

Monitoring Activities

Common to ERM and IC	Introduced in IC and Expanded in ERM	Incremental to ERM
• Conducts ongoing and/or separate evaluations • Evaluates and communicates deficiencies		

631 Both frameworks present monitoring activities as helping to ensure that the components of internal control and enterprise risk management continue to function and remain suitable over time. The *Internal Control—Integrated Framework* presents a more current view of monitoring using baseline information and the monitoring of external service providers.

To submit comments on this Public Exposure Draft, please visit the www.ic.coso.org website. Responses are due by November 16, 2012.

Respondents will be asked to respond to a series of questions. Those questions may be found on-line at www.ic.coso.org and in a separate document provided at the time of download. Respondents may upload letters through this site. Please do not send responses by fax.

Written comments on this exposure draft will become part of the public record and will be available on-line March 31, 2013.