Committee of Sponsoring Organizations of the Treadway Commission

Internal Control—Integrated Framework

Framework

December 2011

To submit comments on this Public Exposure Draft, please visit the **www.ic.coso.org** website. Responses are due by March 31, 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 the exposure draft will become part of the public record and will be available on-line until December 31, 2012.

Draft for Public Exposure

Internal Control—Integrated Framework

Framework

December 2011

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 March 31, 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 the exposure draft will become part of the public record and will be available on-line until December 31, 2012.

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
American Institute of Certified Public Accountants	Charles E. Landes
Financial Executives International	Marie N. Hollein
Institute of Management Accountants	Jeffrey C. Thomson
	Sandra Rictermeyer
The Institute of Internal Auditors	Richard F. Chambers

PwC
Author

Principal Contributors

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

Advisory Council

Sponsoring Organizations Representatives

Audrey A. Gramling	Kennesaw State University	Professor
Steven Jameson	Community Trust Bank	Executive Vice President and Chief Internal Audit & Risk Officer
Steve McNally	Campbell Soup	Finance Director/Controller - Napoleon Operations
Ray Purcell	Pfizer	Director of Financial Controls
Bill Schneider, Sr.	AT&T	Director of Accounting

Members at Large

Jim DeLoach	Protiviti	Managing Director
John Fogarty	Deloitte	Partner
Trent Gazzaway	Grant Thornton	Partner
Cees Klumper	GAVI Alliance	Director of Internal Audit
Thomas Montminy	PwC	Partner
Al Paulus	E&Y	Partner
Tom J. Ray	KPMG	Partner
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	Senior Policy Analyst
Christian Peo	Securities and Exchange Commission	Professional Accounting Fellow
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
Glenn Brady	Partner	St. Louis, USA
Jeffrey Boyle	Partner	Tokyo, Japan
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	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
Alan Martin	Partner	Frankfurt, Germany
Pat McNamee	Partner	Florham Park, USA
Jonathan Mullins	Partner	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
Sachin Mandal	Director	Florham Park, USA
Christopher Michaelson	Director	Minneapolis, USA
Lisa Reshaur	Director	Seattle, USA
Tracy Walker	Director	Bangkok, Thailand

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)

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 now widely used around the world. It is recognized as a leading framework for designing, implementing, and evaluating the effectiveness of internal control.

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

3 COSO believes this 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. COSO is pleased to present this *Internal Control—Integrated Framework* (*Framework*).

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 broad criteria used to assess the effectiveness of an internal control system also remain unchanged. This *Framework* continues to emphasize the importance of management judgment in the design, application, and assessment of effectiveness of a system of internal control.

5 At the same time, the *Framework* now includes important enhancements designed to clarify concepts and ease use and application. One of the most significant enhancements is the codification of internal control concepts introduced in the original framework into principles and attributes. These principles and attributes provide clarity for the user in the design and development of systems of internal control. Principles and attributes can also be used to support the assessment of the effectiveness of internal control. Other updates and enhancements to the *Framework* help the user address changes in business and operating environments, including:

- Expectations for governance oversight.
- Globalization of markets and operations.
- Changes in business models.
- 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 corruption.

6 We are pleased to present this *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, and regulators. The second volume, the *Framework*, defines internal control and describes components of internal control including the underlying principles and attributes. This volume also provides direction for all levels of management to use in designing, implementing, conducting, and evaluating internal control. The third volume, *Evaluation*, provides guidance that may be useful in evaluating the effectiveness of internal control.

7 In addition, a supplemental guide to be published concurrently with the *Framework* focuses the discussion on internal control over external financial reporting, providing practical approaches and examples supporting the preparation of published financial statements. COSO may, in the future, issue other guidance to provide additional assistance in applying this *Framework*. However, neither the guidance on internal control over external financial reporting nor other future guidance takes precedence over this *Framework*.

8 Finally, the COSO Board would like to thank PwC and the Advisory Council for their contributions in developing the *Framework*. Their full consideration of input provided by many stakeholders and their attention to detail were instrumental in ensuring that the core strengths of the 1992 *Internal Control—Integrated Framework* were preserved, clarified, and strengthened.

Definition of Internal Control

9 The primary purpose of this publication, *Internal Control—Integrated Framework* (*Framework*) is to help management better control the organization, and provide a board of directors[1] with an added ability to oversee internal control. Implementing 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. It promotes efficiency and effectiveness of operations, and supports reliable reporting and compliance with laws and regulations.

10 A secondary purpose of this *Framework* is to provide clarity on internal control by using a common definition and integrating various internal control concepts into a framework that defines the components of internal control. It is designed to assist management and other interested parties in assessing the effectiveness of an entity's system of internal control and reporting.

Understanding Internal Control

11 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 in the following categories:*
>
> - *Effectiveness and efficiency of operations.*
> - *Reliability of reporting.*
> - *Compliance with applicable laws and regulations.*

12 This definition emphasizes that internal control is:

- *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 manuals, systems, and forms, but about people at every level of an organization that impact internal control.
- Able to *provide reasonable assurance*, not absolute assurance, to an entity's senior management and board.
- *Geared to the achievement of objectives* in one or more separate but overlapping categories.
- *Adaptable to the entity structure*.

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

13 This definition of internal control is intentionally broad for two reasons. First, it captures key concepts fundamental to how companies and other organizations design, implement, conduct, and evaluate internal control, providing a basis for application across various types of organizations, industries, and geographic regions. It also provides flexibility in application, allowing an entity to sustain internal control for an entire entity, or a subsidiary, division, operating unit, or function relevant for operations, reporting, or compliance objectives, based on the entity's specific needs or circumstances.

14 Second, the definition accommodates subsets of internal control. 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.

A Process

15 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 business. Embedded within this process are policies and procedures. These policies reflect management's statement of what should be done. Such statements may be documented, explicitly stated in other management communications, or implied through management's decisions. Procedures consist of actions that implement a policy. These policies and procedures exist to effect control.

16 Business processes, which are conducted within or across operating units or functional areas, are managed through the fundamental management activities of planning, executing, and checking. Internal control is integrated with these processes. Internal control is most effective when it is embedded in the entity's infrastructure and its ongoing activities.

17 Building in controls to an existing system, or modifying controls elsewhere in the entity, directly affects the entity's ability to reach its goals, supports quality business initiatives, and has important implications to cost. In contrast, layering on new procedures to address internal control separate from those that run the business can add costs. By focusing on existing controls that contribute to the overall system of control, and by building controls into basic operating activities, an entity often can avoid costs of developing new procedures.

Effected by People

18 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 control mechanisms in place.

19 The organization consists of people including the board of directors, senior management, and other personnel. Included among the board's oversight responsibilities are providing advice, counsel, and direction to management, approving certain transactions

2 Although referred to as a process, internal control may be viewed as many processes.

and policies, and monitoring management's activities. Consequently, the board of directors is an important element of internal control. For example, the board and senior management establish the tone for the organization concerning the importance of internal control and expected standards of conduct across the entity.

20 However, people do not always understand, communicate, or perform consistently. Each individual brings to the workplace a unique background and technical 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 objective, 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 duties and the way in which these duties are carried out, and aligned with the entity's objectives.

Provides Reasonable Assurance

21 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.

22 Reasonable assurance does not imply that an entity will always achieve its objectives. The cumulative effect of 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 two or more 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.

Geared to the Achievement of Objectives

23 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 operations and financial performance goals and safeguarding assets against loss.
- *Reporting Objectives*—These pertain to the reliability of reporting. They include internal and external financial and non-financial reporting.
- *Compliance Objectives*—These pertain to adherence to laws and regulations to which the entity is subject.

24 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.

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

26 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 a business to fail to achieve operations goals. For these objectives, the internal control system 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.

Adaptable to the Entity Structure

27 Entities may be structured along various dimensions. The management operating model may follow product or service lines; reporting may be done for an overall consolidated entity, division, or operating unit, with geographic markets providing for further subdivisions or aggregations of performance. The management model may also rely on relationships with external parties to support the achievement of objectives.

28 The legal entity structure is typically designed to follow regulatory reporting requirements, empower managers at foreign operations, limit business risk, or provide tax benefits. Often, the organization of legal entities is quite different from the management structure that is used to run the business.

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

Overview of Internal Control

Introduction

30 An organization establishes a mission, sets strategies, establishes the 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, providing reliable reporting to stakeholders, recruiting and retaining motivated and competent employees, achieving and maintaining a positive reputation within the business and consumer communities, and complying with laws and regulations.

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

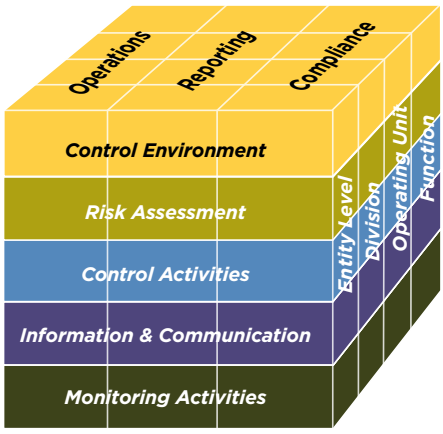
- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring Activities

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

Relationship of Objectives, Components, and the Entity

33 A direct relationship exists between objectives, which are what an entity strives to achieve, the components, which represent what is needed to achieve the objectives, and the operating units, legal entities, and other structures within the entity. 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 organizational 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 this *Framework*, the term "the entity and its subunits" refers collectively to the overall entity, divisions, subsidiaries, operating units, or functions.

34 Each component cuts across and applies to all three categories of objectives. For example, establishing and executing policies and procedures to ensure that management plans, programs, and other directives are carried out—representing the control activities component—is relevant to all three objectives categories.

35 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.

36 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.

37 Internal control is a dynamic and iterative 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 information and communication needs, or its monitoring activities. Thus, internal control is not a linear process where one component affects only the next. It is a dynamic and iterative process in which almost any component can and will influence another.

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

Objectives

39 Management sets entity-level objectives that align with the entity's mission and value proposition. These high-level objectives reflect management's choice of how the organization will seek to create, preserve, and realize value for its stakeholders. Such objectives may be based on the entity's unique operations needs, on laws, regulations, and standards imposed by external parties, 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. Management needs to understand the overall strategies set by the organization. As part of internal control, management specifies objectives that have been set so that risks to the achievement of those objectives can be identified and assessed.

40 Individuals who are part of the internal control process need to understand the overall strategies and objectives set by the organization. As part of internal control, management specifies objectives that have been set so that risks to the achievement of those objectives can be identified and assessed. Specifying objectives relates to the articulation of specific, measurable, attainable, relevant, and time-bound objectives. In most instances, specifying objectives requires some form of codification. However there

may be instances where an entity might not explicitly state an objective. By specifying objectives in appropriate detail, they can be readily understood by the people who are working toward achieving them.

Categories of Objectives

41 This *Framework* groups entity objectives into the three categories of operations, reporting, and compliance.

Operations Objectives

42 Operations objectives relate to achievement of an entity's basic mission—the fundamental reason for its existence. These objectives vary based on management's choices relating to structure, industry considerations, and performance of the entity. Entity-level objectives cascade into related sub-objectives for operations within the divisions, subsidiaries, operating units, and functions, directed at enhancing effectiveness and efficiency in moving the entity toward its ultimate goal. As such, operations objectives may relate to improving quality (i.e., avoiding waste and rework), reducing costs and production time, improving innovation, and improving customer and employee satisfaction.

Reporting Objectives

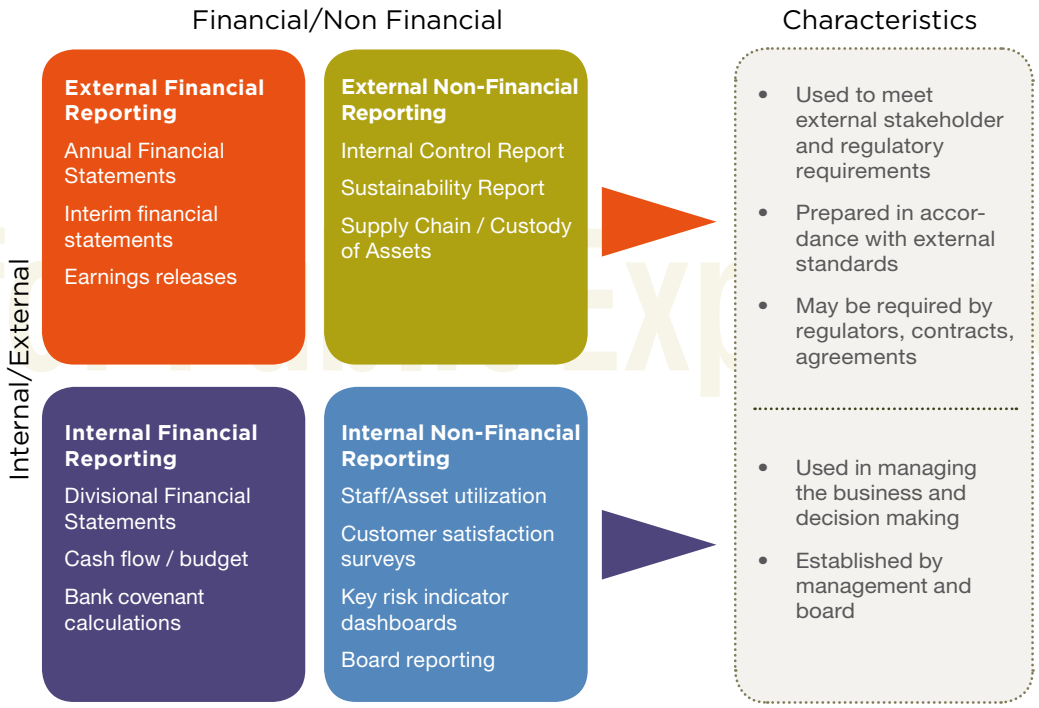
43 Reporting objectives pertain to the preparation of reliable reports. Reporting objectives may relate to financial or non-financial reporting and to internal or external reporting. Internal reporting objectives are driven by internal requirements in response to a variety of potential needs such as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

- *External Financial Reporting Objectives*—Entities need to achieve external financial reporting objectives to meet obligations. Reliable financial statements are a prerequisite to accessing capital markets and may be critical to the awarding of contracts or to dealing with suppliers. Investors, analysts, and creditors often rely on an entity's financial statements to assess performance against peers and alternative investments. Management reporting on the effectiveness of internal control over external financial reporting is part of external non-financial reporting objectives referenced below.
- *External Non-Financial Reporting Objectives*—Management may report external non-financial information in accordance with regulations, standards, or frameworks, including reporting on internal control and operational processes. For example, where management operates in accordance with the International Organization for Standardization (ISO) standards for quality management, it may report publicly on its operations. An entity may engage an independent auditor to review and/or report on its conformance with standards published by such organizations. The entity typically attains an annual certification that demonstrates adherence to such a standard.

- *Internal Financial and Non-Financial Reporting Objectives*—Reliable internal reporting provides management with information needed to manage the organization. It supports management's decision making and assessment of the entity's activities and performance. Internal reporting objectives are based on preferences, judgments, and management style. Internal reporting objectives vary among entities because different organizations have different strategic directions, operating plans and expectations.

Relationship within Reporting Category of Objective

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



45 Reporting objectives are separate and distinct from the information and communication component of internal control. Reporting objectives focus on reliable reporting, and to achieve this, the organization applies all five components of internal control. For instance, an organization in preparing an internal non-financial report to the board on the status of merger integration efforts assigns competent individuals, assesses risks relating to the understandability, relevance, and usefulness of the report, develops controls to address the reliability of the information being reported, and monitors the overall system of internal control supporting this non-financial reporting objective. In contrast, the information and communication component supports the functioning of all components of internal control and the achievement of the reporting category 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 is only part of the overall system of internal control.

Compliance Objectives

46 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 internal control over financial reporting and environmental compliance, but others may be more obscure, such as those that apply to an entity conducting operations in a remote foreign territory.

Basis of Objectives Categories

47 Certain objectives are derived from the regulatory environment or industry in which the business 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.

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

48 Conversely, operations objectives and internal reporting are based more on preferences, judgments, and management style. They vary widely among entities simply because informed and competent people may select different objectives. For example, for product development, one organization might choose to be an early adopter, another might be a quick follower, and yet another a late adopter. These choices will affect the structure, skills, staffing, and controls of the research and development function. Consequently, no one formulation of objectives can be optimal for all entities.

Overlap of Objectives Categories

49 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 timely filings with regulatory agencies. The category in which an objective falls can sometimes vary depending on the circumstances. 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 the reliability of reporting where inventory losses are detected following 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 ensure reliable reporting.

Objectives and Sub-Objectives

50 Management links specified entity-level objectives to more specific sub-objectives that cascade throughout the organization. These sub-objectives also are established as part of or flowing from the strategy-setting process, and relate to subsidiaries, divisions, operating units and functional activities, including business processes such as sales, production, engineering, marketing, productivity, employee engagement, innovation, and information technology. Throughout this process, management ensures that the sub-objectives remain aligned with entity-level objectives and are coordinated across the entity.

51 Where entity-level objectives are consistent with prior practice and performance, the linkage among activities is usually known. Where, however, objectives depart from an entity's past practices, management addresses the linkages or accepts increased risks. For example, an objective to fill more management roles internally through promotions will depend heavily on linked sub-objectives dealing with succession planning, appraising, training, and development. These sub-objectives might be substantially changed if past practice relied heavily on external recruiting.

52 Sub-objectives for operating units and functional activities also need to be clear. These sub-objectives also need to be specific, measurable, 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.

53 Many entities establish multiple sub-objectives for each activity, flowing both from the entity-level objectives and from standards relating to the established compliance and reporting objectives. For procurement, for example, operations objectives may be to:

- Purchase goods that meet established engineering specifications.
- Purchase goods from companies that meet the entity's environmental, health, and safety specifications as set forth in a code of conduct (e.g., no child labor, good working conditions).
- Negotiate acceptable prices and other terms.

Components of Internal Control

54 This *Framework* sets out five components of internal control. It also sets out seventeen principles representing the fundamental concepts associated with each component. All seventeen principles apply to each category of objective, as well as to individual objectives within a category. Supporting the seventeen principles are eighty-one attributes, representing characteristics associated with the principles.

55 Below is a summary of each of the five components of internal control and the principles relating to each. This listing of principles is not meant to imply a binary checklist. Rather, principles are meant to enable effective operation of the components and the overall system of internal control, with appropriate use of management judgment.

56 Each of the principles and attributes is covered in the following chapters. Each principle is introduced at the beginning of the relevant chapter and then presented at the end of the relevant chapter along with the attributes relating to each principle. Attributes are also called out in sidebars to the text of each chapter. For purposes of this *Framework*, in describing these principles and attributes we use the word "organization" to capture the meaning of, collectively, the board, management, and other personnel.

Control Environment

57 The control environment is the foundation for all other components of internal control. The board and senior management establish the tone from the top regarding the importance of internal control and expected standards of conduct. The control environment provides discipline, process, and structure.

58 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 of management and exercises oversight for 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

59 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.

60 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

61 Control activities are the actions established by policies and procedures to 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 and at various stages within business processes, and over the technology environment.

62 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 as manifested in policies that establish what is expected and in relevant procedures to effect the policies.

Information and Communication

63 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 all personnel to understand internal control responsibilities and their importance to the achievement of objectives.

64 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

65 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.

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.

• • •

66 In addition to the five components of internal control noted above, the *Framework* includes discussion recognizing that while internal control provides important benefits, limitations do exist. Limitations result from:

- The quality and suitability of objectives established as a precondition to internal control.
- The realities that human judgment in decision making can be faulty.
- Knowing that decisions on responding to risk and establishing controls must consider the relative costs and benefits.
- Breakdowns that can occur because of human failures such as simple errors or mistakes.
- Controls that can be circumvented by collusion of two or more people.
- The ability of management to override internal control decisions.

67 These limitations preclude the board and management from having absolute assurance of the achievement of the entity's objectives – that is, controls provide reasonable but not absolute assurance.

68 The remaining chapters of this volume, including Roles and Responsibilities and appendices, are not a part of the *Framework*.

Internal Control and the Management Process

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

- Having a board comprised of directors with sufficient independence from management that carries out its oversight role effectively is a part of internal control. However, many decisions reached by the board are not part of internal control; for example, deciding on or approving a particular strategic plan. The board will fulfill a variety of governance responsibilities that are in addition to its responsibilities for oversight of internal control.
- Setting objectives is part of or flows from the broader strategic planning process. Ensuring that management specifies the objectives chosen by the entity is part of internal control; however, the appropriateness of particular objectives selected is not.
- Setting the overall level of acceptable risk and associated risk appetite[4] 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 not part of internal control.
- Developing control activities that contribute to the mitigation of risks based on a risk assessment process is a part of internal control, but choosing which risk response is preferred to address specific risks is not.

Assessing Effectiveness

70 An effective system of internal control provides reasonable assurance regarding achievement of an entity's objectives. To have an effective system of internal control relating to one, two, or all three categories of objectives each of the five components must be present and operate together in a manner that reduces, to an acceptable level, the risk of not achieving an objective.[5] Further, the existence of any material weakness (with respect to external financial reporting objectives) or major non-conformity (with respect to operations, compliance, or non-financial reporting objectives) would preclude an organization from concluding that the entity's system of internal control is effective. For example, effective internal control over a particular compliance objective requires that all five components be present and operating together.

71 Effectiveness of internal control is assessed relative to the five components of internal control. Determining whether an overall system of internal control is effective is a subjective judgment resulting from an assessment of whether each of the five components of internal control are present and whether the five components of internal control are operating together. Because internal control is relevant to an entire entity and its subunits, effectiveness of internal control can also be assessed relative to a specific part of the organizational structure.

4 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.

5 The phrase "present and operating together in a manner that reduces, to an acceptable level, the risk of not achieving an objective" is subsequently referred to as "present and operating together".

72 When internal control is determined to be effective for each of the three categories of objectives, management and the board of directors have reasonable assurance, relative to the application within the entity structure, that the organization:

- Understands the extent to which operations are managed effectively and efficiently.
- Prepares reliable reports.
- Complies with applicable laws and regulations.

73 Evaluating each component of internal control requires consideration of how it is being applied by the entity within the system of internal control, and not whether it is effective on its own. Components should not be viewed discretely. Rather the components should be viewed as an integrated system working together to attain effective internal control. The notion that all five components of internal control must be present and operate together does not mean that each should function identically, or even at the same level, in different entities. Different entities' internal control systems can operate differently.

74 Furthermore, the integration of these five components is important in assessing the effectiveness of a system of internal control. Because controls can serve a variety of purposes, controls put in place to effect principles in one component can serve a purpose that may also apply to another component. Controls exist in each of the five components of internal control. Additionally, controls can differ in the degree to which they address a particular risk, so that the portfolio, or combination of controls, each with limited effect, together can act satisfactorily in reducing risks to the achievement of objectives.

75 Any change in the application of one component should not be viewed in isolation. That is, changes in one component require an evaluation of the potential effects and need for changes in other components. Thus, the contributions made by each component as well as the five components together are evaluated in determining whether a system of internal control is effective.

Considering the Principles in Assessing Effectiveness

76 In assessing whether the system of internal control is effective, senior management and the board of directors determine to what extent the principles and, in turn, the corresponding attributes associated with each component are present and functioning.[6] This evaluation entails considering how the principles and attributes are being applied. Determining whether a principle is present and functioning implies that the organization:

- Understands the intent of the principle and how it is being applied.
- Applies the principle consistently across the entity.
- Works to help personnel understand and apply the principle across the entity.

6 For purposes of this Framework, the phrase "present and functioning" applies to components, principles, and attributes. Present means that a component, principle, or attribute has been implemented. Functioning means that a component, principle, or attribute is operating as intended.

- Views omission of or non-conformity with a principle as an exception (i.e., not applying the wording, intent, and spirit of the principle is the exception rather than the norm).

77 Furthermore, a principle that is present and functioning operates within a range of acceptability and does not imply that the organization achieves the highest level in applying the principle. Management must still be able to assess the trade-offs between the cost of achieving perfection and the benefits of seeking to operate at the highest levels of sophistication and capability.

78 When a principle is deemed not to be present or functioning, an internal control deficiency exists. Management applies judgment in evaluating whether a deficiency prevents the entity from concluding that a component of internal control is present and functioning. These judgments may vary depending on the category of objectives, and additional considerations relating to deficiencies in internal control over operations, compliance, financial reporting, and other reporting are considered in the following sections.

79 Even though attributes are expected to be present and functioning, it may be possible to determine that the corresponding principle is present and functioning, and thus a component can be present and functioning without every attribute being present. For instance, management may be able to determine that Principle 1, "The organization demonstrates a commitment to integrity and ethical values" is present and functioning based on an assessment that only three of the four related attributes are present and functioning. The organization may set the tone at the top, evaluate adherence to standards of conduct, and address deviations in a timely manner, but it does not formally define the expectations of management and the board of directors in the entity's standards of conduct. However, in the absence of an attribute being present and functioning, a deficiency may still exist.

Deficiencies in Internal Control

80 Deficiencies in an entity's system of internal control may surface from many sources, including the entity's monitoring activities and other components of internal control, and external parties that provide input relative to the operation of a component.

81 The term "deficiency" refers to a shortcoming in some aspect of the system of internal control and has the potential to adversely affect the ability of the entity to achieve its objectives. When an organization determines that a deficiency exists, management needs to assess the impact of that deficiency on the effectiveness of the entity's system of internal control. Further, the responsibility for identifying and assessing deficiencies rests with the organization, in the normal course of performing the functions. Certain external parties, such as external auditors and regulators, are not part of the system of internal control and cannot be relied upon to detect and assess deficiencies.

82 Not every deficiency will result in a conclusion that an entity does not have an effective system of internal control. For one thing, other controls may be present and functioning that allow for each of the components to be present and for all five components to be operating together. When a deficiency is noted, the evaluator considers the effect of controls in the same or other components.

83 Assessing the severity of a deficiency or combination of deficiencies to determine the potential impact on the system of internal control requires judgment. This *Framework* sets forth the criteria through the components, principles, and attributes for management to assess the effectiveness of an entity's system of internal control and to determine and assess the nature of a deficiency. Management may decide or be required to consider additional criteria established by external parties for evaluating and classifying the severity of a deficiency or combination of deficiencies. For example, regulators, standard-setting bodies, listing agencies, and other relevant third parties have established additional criteria contained in standards and other guidance for evaluating the classification of deficiencies relating to the external financial reporting objective and to non-financial reporting, operations, and compliance objectives discussed in the next sections. This *Framework* does not prescribe such additional criteria, but recognizes and accommodates the authority and responsibility of those external parties to issue rules and guidance for such classifications.

Deficiencies in Internal Control over Financial Reporting

84 There are specific considerations when a deficiency relates to internal control over financial reporting. In this case, three tiers of deficiencies are commonly used: deficiency, significant deficiency, and material weakness.

85 For the purposes of this *Framework*, material weakness is considered in relation to an entity's financial reporting objective, and is defined as a condition in which there is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, detected, or corrected on a timely basis. Determining when a material weakness exists requires applying judgment which includes several considerations, such as:

- The likelihood that a potential material misstatement exists and will not be prevented or detected and corrected in a timely manner.
- The magnitude of the potential or actual misstatement in relation to the entity's financial statements.

86 The above material weakness concept establishes boundaries around effectiveness, which is a threshold of seriousness against which deficiencies are measured. Some regulators or standard-setting bodies may provide other factors for consideration in determining the existence of a material weakness. For external financial reporting, the existence of a material weakness precludes an organization from asserting that the entity's system of internal control over external financial reporting is effective.

87 A significant deficiency is a deficiency or combination of deficiencies less severe than a material weakness, yet may be important enough to merit attention by the board of directors. Multiple significant deficiencies when considered collectively may result in a determination that a material weakness exists.

Deficiencies in Internal Control over Operations, Compliance, and Other Reporting

88 In evaluating deficiencies in internal control over operations, compliance, and non-financial reporting, this *Framework* suggests classifying such deficiencies as major and minor non-conformities.[7] A major non-conformity refers to any deficiency in internal control that relates to compliance, operations, and non-financial reporting activities that adversely affects the likelihood that the entity will achieve its objectives. For operations, compliance and non-financial reporting, the existence of any major non-conformity precludes an organization from concluding that the entity's system of internal control over these objectives is effective. For instance, a major non-conformity may exist when a deficiency in internal control has the potential for:

- Shipping a nonconforming product—e.g. a product that does not meet quality requirements.
- Making unauthorized significant changes to product design and manufacturing specifications.
- Not completing routine maintenance of assets, especially those that relate to public safety (e.g., aircraft, railways, or public transit).
- Administering improper medicine doses to hospital patients.
- Recurring misreporting of incidences of non-compliance to regulators.
- Omitting important information supporting budgeting and forecasting activities.
- Improperly treating, storing, or disposing of hazardous wastes.
- Improperly reporting child labor found to be occurring at own or supplier's factories.
- Improperly reporting CO_2 emissions to customers and investors.
- Acquiring incomplete or inaccurate data for use in actuarial valuations.
- Making unauthorized significant changes to health and safety specifications.

89 A minor non-conformity refers to any deficiency relating to compliance, operations, and non-financial reporting activities that does not adversely affect the likelihood that the entity will achieve its objective. For instance, a minor non-conformity may exist when a deficiency in internal control has the potential for:

- Failing to document a part of the quality system.
- Not inspecting an instrument past its calibration date.
- Failing to conduct routine maintenance of an asset needed to keep a warranty in effect.

7 Some standard-setting bodies and governmental agencies use the term material weakness to refer to major conformities. For instance, the Auditing Standards Board of the AICPA defines a material weakness in internal control over compliance as a deficiency, or combination of deficiencies, in internal control over compliance such that there is a reasonable possibility that material noncompliance with a compliance requirement will not be prevented or detected and corrected on a timely basis.

- Filing a compliance statement with a regulator one day after the required filing date.
- Not retaining a training record for future reference.
- Using inaccurate data to prepare management information for internal analysis.

90 Multiple minor non-conformities when considered collectively may result in a determination that a major non-conformity exists.

Other Considerations for Internal Control

Organizational Boundaries

91 Increasingly, many organizations are choosing to shift business activities to outside service providers. Such an 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.

92 Outsourcing, strategic sourcing, and other outside 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 opportunities for cost savings 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.

93 Using outsourcing, strategic sourcing, and other outside service providers can provide substantial benefits of speed, efficiency, and costs savings to an entity, and the trend to outsourcing is likely to grow. This dependence on external parties 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 activities and the related internal controls. While management can use others to execute activities for or on behalf of the entity, it cannot abdicate responsibility to monitor those activities, manage the associated risks, and establish mechanisms to support the functioning of the components of internal control.

94 This *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

95 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 will the extent that technology is used in most entities.

96 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, computer hardware and software, methodologies, and processes. This *Framework* uses the term "technology" to refer to all computerized systems, including software applications running on a computer and operational control systems.

97 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, geographies, processes, and technologies. 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.

98 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.

99 The principles presented in this *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. Because technology is continually evolving, this *Framework* does not address specific technologies, such as cloud computing or the rise in social media.

Larger versus Smaller Entities

100 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 a publicly traded company, a privately held entity, a government organization, or a not-for-profit organization. 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 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.

101 Smaller entities typically have unique advantages over larger ones 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.

102 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 company's economic resources than would be the case for a larger multinational entity. Certainly, the smaller company's internal audit function would be smaller, and might rely on co-sourcing or outsourcing in order to provide needed skills, where the larger company's function might be significantly larger with a broad range of experienced in-house personnel. But in all likelihood the relative cost for the smaller company would be higher than for the larger one.

Benefits and Costs of Internal Control

Benefits

103 Internal control provides many benefits to an entity. It provides management and the 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 criteria required to access the 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.

104 Other benefits of effective internal control include:

- Reliable and relevant information supporting management's 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.

- Retention of the facts, reasoning, and 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.

105 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

106 Generally, it is easier to deal with the cost aspect in the cost-benefit equation because in most cases 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. 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

107 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. For example, 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. 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.

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

109 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 the ultimate actions it 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

110 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 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 tool 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 external parties, such as regulators, auditors, or customers.

111 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. As well, 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 will require 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 will or should be more formal, but that sufficient evidence that the components of internal controls are present and *operating together* is available and suitable 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 would include evidence that the system of internal controls is properly designed and *operating effectively*. In considering the nature and extent of documentation needed, management should also 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 may also document significant judgments, how such decisions were considered, and the final decisions reached.

112 There may still be instances where internal controls are 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.

113 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. Smaller companies often find less need for formal documentation, such as in-depth policy manuals, flowcharts of processes, organization charts, and job descriptions. 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. In a smaller business, management is often directly involved in performing control procedures for which there may be only minimal documentation because management can determine that controls are functioning through direct observation.

114 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.

Control Environment

Chapter Summary:

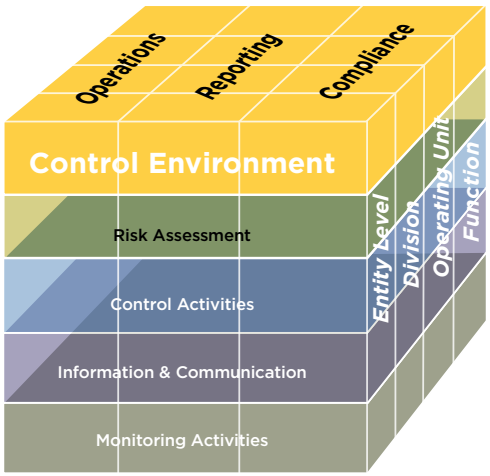
115 The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The board of directors and senior management establish the tone at the top regarding the importance of internal control including expected standards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

116 The control environment is the foundational component of internal control, 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 various levels in carrying out their responsibilities for internal control and making decisions in the pursuit of the entity's objectives. 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.



117 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 behaviors of 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. In both the short and long term, it positions itself to be more resilient in the face of internal and external pressures.

118 Control environment is sometimes seen as synonymous with internal control culture, in that the elements that make one strong, such as integrity and ethical values, oversight, accountability, and performance evaluation, make the other strong as well. 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.

Principle 1.

Demonstrates Commitment to Integrity and Ethical Values

The organization demonstrates a commitment to integrity and ethical values.

Tone at the Top and throughout the Organization

119 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 in the pursuit of the entity's objectives. Such values balance the needs and concerns of different stakeholders, such as employees, suppliers, customers, competitors, regulators, investors, and the wider community. For example, in addition to fostering understanding and adherence to legal and regulatory requirements, management and the board may seek to set the tone in terms of moral, social, environmental, or other forms of responsible conduct. 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.

120 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 the board of directors, all employees, outsourced service providers, and business partners. They may also include voluntary responsible conduct, such as carbon footprint awareness, community outreach after natural disasters, and other activities. 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.

121 Tone is impacted by the personal conduct of management and the board of directors, even when the behavior does not directly affect the achievement of the organization's objectives. Consider, for instance, the adverse effect of fraudulent or questionable practices, such as insider trading activity, personal indiscretions, lack of receptiveness to bad news, or compensation practices so unfairly balanced that they could incent inappropriate conduct. In contrast, a history of ethical and responsible behavior by management and the board of directors sends a strong message 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 can be influenced by the knowledge that the chief executive officer has done the right thing ethically when faced with a tough business-based or personal decision.

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

123 In some cases, the tone set by the chief executive may result in unintended consequences when considering the various objectives of the entity. 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 generating revenue or operating efficiently and effectively—for instance getting products to customers faster—it may be detrimental to the achievement of other objectives, such as complying with product safety standards, quota violations, fair sales practices, or other requirements. Clear guidance and direction from the top, and congruence across different levels of management are fundamental to the achievement of the entity's objectives. Therefore tone can be either a driver or a barrier to internal control.

Standards of Conduct

124 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 governing laws, regulations, other standards, and other expectations that the organization's stakeholders may have, such as corporate social responsibility.

125 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. These are translated into an organizational statement of beliefs and values and standards of conduct.

126 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?

127 Organizations include integrity and ethical values in their communications and training. For example, a company that regularly receives awards for "best places to work" and achieves high employee retention rates provides training on corporate ethical values and organizational culture, under the direction of a senior board member. The training sessions are conducted quarterly or biannually depending on the number of new employees hired. During the 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.

128 The organization's standards of conduct are communicated and reinforced not only at all levels of the organization but also at outsourced service providers. For example, enforcement of 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.

129 Management that delegates through legal or contractual arrangements the execution of certain activities to outsourced service providers retains ultimate accountability for those activities. 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.
- The competency of the service provider.
- The entity's existing knowledge of controls.
- The magnitude and level of complexity of the entity's supply chain and business model.

130 Inappropriate conduct by outsourced service providers or business partners can reflect negatively upon senior management and impact the entity itself by causing harm to customers or 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

131 The established standards of conduct provide the basis for evaluating adherence to integrity and ethical values across the organization and its outsourced service providers. These are communicated through the organization's set of 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, it is the actions, decisions, and attitudes of individuals that require oversight and evaluation.

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

- Tone at the top 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 that leaves senior management unaware of actions taken at lower levels.
- Inadequate vehicles by which employees can safely voice questions and concerns.
- Failure to address non-existence 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 insignificant or unpublicized and thus lose their deterrent value.

133 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 further determines the tolerance level for deviations. Certain expected standards of conduct may be deemed zero tolerance for deviations, while others may be deemed addressed with warnings to personnel.

134 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., 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.

135 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.

136 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.

Principle 2.

Exercises Oversight Responsibility

The board of directors demonstrates independence of management and exercises oversight for the development and performance of internal control.

Authorities and Responsibilities

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

138 The board, in turn, charges the chief executive officer with overall execution of the entity's strategy and achievement of its objectives, supported by an effective system of internal control. The board has the authority to assign responsibilities, probe management, retain key decision-making authority, and follow up on resolution of issues as necessary. Determining the appropriate delegation of authorities and responsibilities to individuals with the right skills and expertise is essential to the entity's ability to achieve its objectives.

139 Depending on the jurisdiction, oversight structures are developed voluntarily or as mandated by law, regulation, or standards, such as stock exchange listing standards. While smaller companies may require less extensive governance structures, larger public companies may need 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 management's integrity and transparency in external reporting and overall reliability of financial reports.
- Other committees of the board dedicated to address specific matters that are critical to the entity's objectives (e.g., compliance committees for pharmaceutical companies).

140 In addition to board-level oversight, senior management establishes similar structures and processes on 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 implications for the internal control system.

141 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 in making decisions, designing controls, and evaluating performance. 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 processes and controls most suitable to its business activities.

Independence and Relevant Expertise

142 The board of directors demonstrates independence of management and relevant skills and expertise in carrying out its oversight responsibilities. Independence requires there to be no personal or professional relationship with or allegiance to the entity in order to allow for an unbiased and impartial mindset.[8] This includes consideration of the various board seats held by each of the board members and limiting any bias or conflict of interest that could result from board members sitting on each other's companies' boards.

143 Because a board must be prepared to question and scrutinize management's activities, present alternative views and have the courage to act in the face of obvious wrongdoing, it is necessary that the board contain outside directors. Certainly, officers and employees often are highly effective and important board members, bringing knowledge of the company to the table. But there must be a balance. Although smaller companies or government entities may find it costly or otherwise difficult to attract a majority of outside directors—usually not the case with large organizations—it is important that the board contain at least a critical mass of outside directors. The number should suit the entity's circumstances, but more than one outside director normally is needed for a board to have the requisite balance. Those entities that are unable to have an independent board recognize this factor and evidence the processes and structures that facilitate adequate oversight of the entity.

144 Board members whose livelihood does not depend on the entity's performance are generally able to provide unbiased evaluations and guidance. Consider, for example, a company that has a board member whose regular occupation is that of a professor at a small university and whose compensation as a board member of the company comes close to or exceeds his regular pay. As a result, he is highly motivated to retain his board position and may be softer in challenging management and evaluating its performance. Indeed, the bias created by the relative significance of board compensation can jeopardize the independence of members.

145 Board composition considers the mission, values, and various objectives of the entity as well as the skills and expertise needed to guide, probe, and evaluate the senior management team most appropriately. The board of directors includes members that collectively represent the requisite skills and expertise, with sufficient overlap to enable discussion and deliberation. Skills and expertise are typically expected to include:

- Market and company 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).

8 Consider for example the New York Stock Exchange Corporate Governance Rules of 2003 that state that "No director qualifies as 'independent' unless the board of directors affirmatively determines that the director has no material relationship with the listed company (either directly or as a partner, shareholder or officer of an organization that has a relationship with the company)."

- Ethical standards (e.g., ability to identify and resolve ethical dilemmas).
- Leadership and strategic thinking (e.g., ability to make informed decisions in the interest of the entity, considering a multitude of stakeholders).
- 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).
- Problem-solving and investigation (e.g., training and experience in identifying and resolving issues).

146 The expertise, skills, and independence of the board of directors are evaluated regularly in relation to the evolving needs of the entity. 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 Components	Oversight Activities of the Board
Control Environment	• Provide strategic direction to guide the organization in the achievement of its objectives and viability of the business. • Guide the definition of and adherence to standards of conduct for the organization commensurate with stakeholder expectations. • Guide the definition of standards of conduct, competence, and performance for the organization and use these to regularly evaluate senior management who, in turn, evaluates the organization, outsourced service providers and business partners. • Direct the implementation of an oversight structure that is aligned with the objectives of the entity (e.g., board and committees as necessary). • Exercise fiduciary responsibilities and due care (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 discussions and commensurate actions on these items with management (e.g., for transactions that occur repeatedly at the end of interim or annual reporting periods).
Risk Assessment	• Consider internal and external factors that pose risks to the achievement of objectives; identify issues and trends (e.g., sustainability implications of the entity's business operations). • Review and comment on 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. • Evaluate how proactively the organization manages innovations and changes such as those triggered by new technology or economic and geopolitical shifts.

Internal Control Components	Oversight Activities of the Board
Control Activities	• Provide guidance to senior management on the selection, development, and deployment of control activities. • Oversee the establishment of structures, roles and responsibilities that enable adequate segregation of duties.
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. • Allow for and address upward communication of issues.
Monitoring Activities	• Assess and oversee the nature and scope of monitoring activities and management's evaluation and remediation of deficiencies. • Engage with internal and external auditors to evaluate the level of awareness of strategies, risks, and control implications associated with evolving business, infrastructure, regulations, and other factors.

147 Transparency obligations reinforce accountability of both senior management and the board of directors. While disclosure requirements and expectations differ by jurisdiction, industry, and other factors, 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 governance process to deal with planned and unplanned issues.

Principle 3.

Establishes Structure, Authority, and Responsibility

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

Organizational Structures and Reporting Lines

148 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. The goal is to provide for clear accountability and information flows within and across the overall entity and its subunits.

149 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, 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 external parties to support the achievement of objectives which creates additional structures and reporting lines.

150 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.

151 Organizational structures evolve as the nature of the business evolves. Management therefore reviews and evaluates the structures for continued relevance and effectiveness 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.

152 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. Variables to consider when establishing and evaluating organizational structures include the following:

- Size and nature 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" vs. secondary report/"dotted line") and communication channels.
- Structures that are needed to satisfy the organization's objectives (e.g., local market structure, business segment structure, tax optimization model).
- Structure and reporting requirements of relevant jurisdictions.

153 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.

154 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 the second line of defense by offering 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 provides 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 of the business areas they review.

155 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 ration. alization (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

156 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, accountable, consulted, 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.

157 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 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.

158 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 senior management, delegating more authority and responsibility to lower levels, shifting activities to outsourced service providers, 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.

159 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 provide 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

160 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.

Principle 4.

Demonstrates Commitment to Competence

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

Policies and Practices

161 Policies and practices are the high-level guidance and behaviors 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, 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 sharpening the skills of management and other personnel).
- Means to react dynamically to change (e.g., new regulatory requirements, new risks identified, or internal decision to modify business processes are reflected in policies and practices and cascade throughout applicable operating procedures).

162 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 behaviors should be applied.

Commitment to Competence

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

164 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.

165 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.
- Trade-off between the extent of supervision and the requisite competence level of the individual.

166 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, skills, expertise, or a combination of such factors. Management is responsible for acting on such shortcomings in a timely manner.

Attracting, Developing, and Retaining Individuals

167 The commitment to competence is supported by and embedded in the human resource 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 define policies, procedures, 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

168 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

169 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.

170 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.

171 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.

Principle 5.

Enforces Accountability

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

Accountability for Internal Control

172 The board of directors ultimately holds the chief executive officer accountable for internal control in the achievement of the entity's objectives. The CEO and senior management, in turn, are responsible for designing, implementing, conducting, and periodically evaluating whether the defined structures, authorities, and responsibilities establish accountability for internal control at all levels of the organization. Accountability refers to the level of ownership for and commitment to the performance of internal control in the pursuit of objectives. Outsourced service providers may be used to carry out responsibilities together with or on behalf of management, yet accountability for internal control remains with management. For all entity structures and levels of authority and responsibility, accountability for internal control is applied to support day-to-day decision making, attitudes, and actions. Management and the board establish the mechanisms to communicate and hold personnel accountable for their performance of internal control responsibilities across the organization and take appropriate corrective action as necessary.

173 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, business unit, geography, or other existing structural entity.

174 Accountability is interconnected with leadership, insofar as the tone at the top and at various levels of the organization is strong where internal control responsibilities are understood, carried out, and reinforced. Tone helps to establish and enforce accountability 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).

- Management's philosophy and operating style, expressed in the form of the consciousness, formality, persistence and other attitudes of management toward internal control, impacting how the organization treats its employees, customers, suppliers, and the broader community (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 dangerous territory).
- Control and information flow (e.g., how decisions are made and communicated and the extent to which cross-organizational collaboration is enabled).
- Upward and other communications 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).

175 Accountability is driven by tone at the top and supported by the commitment to integrity and ethical values, competence, structure, and other elements of internal control, 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

176 Performance is greatly influenced by the extent to which individuals believe they will be held accountable and compensated fairly.

177 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. To support the entity's short- and long-term objectives, performance measures are 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. The company seeks to reduce its production defect rate and therefore aligns its performance measures, incentives, and rewards with both the operating unit's production goals and the expectations to comply with product safety standards, employee wage laws, or product warranty financial data reporting outcomes.

178 Performance measures, incentives, and rewards support an effective system of internal control insofar as they are adapted to the entity's objectives. The following table illustrates key success measures and considerations:

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. • Define metrics to transform disparate data into meaningful information on performance.
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	• Identify and align performance measures with the significant sources of value creation—and destruction—for the entity. • Measure expected versus actual conduct and the impact of the deviations, both positive and otherwise. • Assess the expected impact of performance on risk, operational improvement, and business performance.
Adjustment to Changes	• Adjust performance measures regularly based on a systematic and continuous evaluation of the potential impacts of risks as these evolve over time as well as the quantification of the associated rewards.

179 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 positive incentives. Management reviews the organization's measurement and reward structures to ensure that they do not create incentives for 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 of conduct). 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.

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

181 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.

182 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

183 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.

184 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 circumvent processes or undertake fraudulent activity or corruption.

185 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.

186 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.

187 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.

188 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 their 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

189 competencies, and timely and accurate reporting to stakeholders as their most critical objectives for the viability of the business. They also recognize and expect management and other personnel as well as 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

190 Just as performance objectives are cascaded down from the board of directors to the chief executive officer, to 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.

191 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 need to be superior to offers from peers in the industry). 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 manage the process of obtaining, processing, and communicating the relevant information to appropriate levels of management and other personnel.

192 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.

Summary of Principles and Attributes Relating to Control Environment

193 Noted below are the five principles and related twenty-one attributes for Control Environment.

Demonstrates Commitment to Integrity and Ethical Values

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

- **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.

Exercises Oversight Responsibility

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

- **Establishes Board of Directors Oversight Responsibilities**—The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations.
- **Retains or Delegates Oversight Responsibilities**—The board of directors retains oversight responsibilities or delegates these to senior management as required to support the achievement of objectives.
- **Applies Relevant Expertise**—The board of directors defines and periodically assesses the essential knowledge and skills 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 of the organization and demonstrate objectivity.

- **Provides Oversight**—The board of directors guides, directs, and reviews the development and performance of the system of internal control:
  - » **Control Environment**—Establishing integrity and ethical values, structure, authority and responsibility, competence, and accountability throughout the organization.
  - » **Risk Assessment**—Reviewing and commenting on 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 guidance to senior management around the selection, development, and deployment of control activities.
  - » **Information and Communication**—Obtaining, reviewing 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.

Establishes Structure, Authority, and Responsibility

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

- **Considers All Structures of the Entity**—Management and the board of directors consider the multiple structures used (including operating units, legal entities, 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, and assign responsibility and segregate duties as appropriate 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.

Demonstrates Commitment to Competence

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

- **Establishes Policies and Practices**—Policies and practices reflect the organization's expectations of competence necessary to support the achievement of objectives.
- **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.
- **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.
- **Plans and Prepares for Succession**—Senior management and the board of directors develop contingency plans for assignments of responsibility important for internal control.

Enforces Accountability

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

- **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.

Risk Assessment

Chapter Summary:

194 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 of operations, reporting, and compliance with sufficient clarity to be able to identify and analyze risks to those objectives. 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.

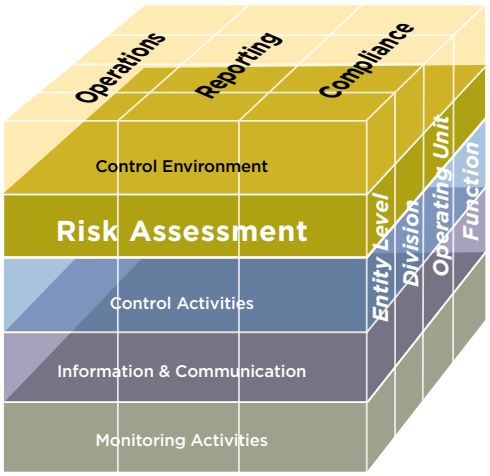
7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

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

195 All entities, regardless of size, structure, nature, or industry, encounter risks at all levels. Risk is defined in this *Framework* as the possibility that an event will occur and adversely affect the achievement of objectives. 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 channel back to the strategy or objective-setting processes. However, identifying and assessing potential opportunities is not a part of internal control.



196 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.

197 A precondition to risk assessment is the establishment of measurable 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 upon 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. Where objectives within these categories are unclear or where it is unclear how these objectives support the strategic direction, management communicates this concern for input to the strategy-setting and objective-setting process.

198 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

199 Risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. Operating within risk tolerance provides management 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, whereas for compliance and operations, risk tolerance is often expressed in terms of the acceptable level of variation in performance.

200 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, regulations, and external standards.

201 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.

202 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, a company:

- 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 24 hours, but accepts that up to 10% of complaints may receive a response within 36 hours.

Principle 6.

Specifies Relevant Objectives

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

Operations Objectives

203 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 measurable criteria. Among its objectives are to, for example:

- Implement public engagement activities for a greenhouse gas reduction program.
- Increase focus on seatbelt use, speeding, impaired driving, and intersection enforcement initiatives.
- Implement water rates relative to industrial and residential consumption patterns.

204 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.
- Lower its CO^2 emissions and reduces and recycles packaging material.
- Broaden the number of vendors to speed up time to market and reduce exposure to loss of supply from any one vendor.

205 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.

206 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.

Reporting Objectives

207 Reporting objectives pertain to the preparation of reliable reports. These reporting objectives may relate to financial or non-financial reporting. This category of objectives includes internal financial reporting, external financial reporting, internal non-financial reporting, and external non-financial reporting. Internal reporting objectives are driven by the entity's strategic directions and by reporting expectations at various levels of the entity. External reporting objectives are driven primarily by rules, regulations, and standards established by governments, regulators, accounting bodies, and other standard-setting organizations.

External Financial Reporting Objectives

208 Entities need to achieve financial reporting objectives to meet external obligations. Reliable financial statements and financial information are a prerequisite to 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.

209 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 reliable financial reports, including published financial statements, financial statements distributed only to specified external users, and financial information derived from an entity's financial or management accounting books and records.

- Published 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. External financial reporting objectives relating to published financial statements are typically established by standards setters and regulators.
- Financial statements distributed only to specified external users may include, for instance, reporting to a bank that has financial covenants established in a loan agreement, to taxing authorities in connection with the filing of tax returns, and to a funding agency by a not-for-profit entity where such statements are not made public. External financial reporting objectives relating to these financial statements are typically driven by standard setters and regulators or by accounting requirements established through contracts and agreements.
- Other financial reporting derived from an entity's financial and management books and records rather than from published financial statements may include earnings releases, selected financial information posted to an entity's website, and select amounts reported in regulatory filings. External financial reporting objectives relating to financial information derived from an entity's financial accounting books and records may not be driven directly by standard setters and regulators, but are typically expected by stakeholders to align with such standards and regulations.

210 External financial reporting reflects underlying 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. One grouping of qualitative characteristics of external financial statements includes:[9,10]

- *Understandability*—allows for reasonable expertise on the part of the users.
- *Relevance*—the ability to influence users' economic decision by helping or confirming the evaluation of events of the past, present, or future. Materiality is a subsidiary concept of relevance.
- *Reliability*—required before information can be useful and requires information to be free of material error and bias.
- *Comparability*—over time and from one entity to another. This requires consistency, and the disclosure of accounting policies and any changes in them.

211 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.[11] With external 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.

212 The term "reliability" as used with external financial reporting objectives involves preparing 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.[12] 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.

213 The qualitative characteristics noted above are applied along with appropriate accounting standards and 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.[13]

9 Derived from International Financial Reporting Standards paragraphs 2.19 through 2.26.

10 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.

11 Derived from International Financial Reporting Standards paragraph 2.26. Some jurisdictions will have other descriptions of materiality.

12 Derived from International Financial Reporting Standards paragraph 2.21.

13 Derived from International Accounting Standards Board (IASB) International Standards on Auditing 315.

External Non-Financial External Reporting Objectives

214 Management may also report information externally consistent with non-financial external standards or frameworks. For example, where management operates in accordance with the International Organization for Standardization (ISO) standards for quality management, it may report publicly on its operations. The entity may have an independent audit conducted and report on the entity's conformance with ISO 9001. 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.

215 As with financial reporting, non-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.

216 As with external financial reporting, other types of external reporting reflect the required level of precision and accuracy suitable for external users' needs and the underlying entity activities, presenting transactions and events within a range of acceptable limits.

Internal Reporting Objectives

217 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. 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.

218 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.

Compliance Objectives

219 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.

220 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 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.

221 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 operations objectives, management considers the acceptable levels of variation in performance within the context of complying with laws and regulations.

Principle 7.

Identifies and Analyzes Risk

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.

222 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.

223 This process is supported by a variety of activities, techniques, and mechanisms, each relevant to the overall risk assessment. Management considers risks at all levels of the entity and takes the necessary actions to manage them. 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

224 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 external parties. These external parties can include potential and existing suppliers, investors, creditors, shareholders, employees, outsourced service providers, 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 the issuance of new laws and regulations, environmental issues, potential natural events, among many others.

225 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 may be addressed by scanning and analyzing relevant risk factors, as remote as they may seem.

Considers Entity, Subsidiary, Division, Operating Unit, and Functional Levels

226 Risk identification considers risks within the overall entity and its subunits, such as finance, human resources, marketing, production, and purchasing. 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

227 Management considers risks in relation to internal and external factors. In conducting these risk assessments, management considers the rate of change in determining the frequency of its risk assessment process. While risk assessment is a dynamic process, organizations will typically use a combination of ongoing and periodic risk assessments. Entities may not continuously consider all risks due to the rate of change, other operational priorities, and cost considerations. However, 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

228 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 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.
- 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.
- 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.

229 Internal factors may include:

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

230 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.

231 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 and quantity, number, 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

232 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.

233 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 not meeting specifications or not being 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.

234 Potential causes of failing to achieve an objective range from the obvious to the obscure and from the significant to the insignificant. 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 a company's production facility, while it may be reasonable to consider in some detail the risk of an airplane crash for a facility located near an airport.

Risk Analysis

235 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

236 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.

Significance of Risk

237 As part of risk analysis, the organization assesses the significance of risks to the achievement of 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.

238 "Likelihood" and "impact" are commonly used terms, although some entities use the terms "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 specificity, 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.

239 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 requirement develop much more slowly than do changes in customer preferences.

240 Management often uses performance measures in determining 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. A company, 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.

241 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 can be more important 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.

Inherent and Residual Risk

242 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.

243 Estimates of significance of the risk often are determined 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. However, even where internally generated data is a primary input, 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. However, using data from past events can provide incomplete conclusions where events occur infrequently.

244 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 short- to mid-term time horizons, management naturally focuses on risks associated with those time frames. However, some objectives extend to the longer term. As a result, management needs to be cognizant of the longer time frames and not ignore risks that might be further into the future.

Risk Response

245 Once the potential significance of risks has been assessed, management considers how the risk should be managed. This involves 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 involve an iterative process.

246 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.

247 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 needed to enable the response to achieve the intended reduction in significance.
- Costs versus benefits of potential responses.

Evaluating Risk Response Options

248 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, a company with a data center located in a region with heavy storm activity 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 does reduce the likelihood of a similar storm occurring near that new location.

249 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

250 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 deemed necessary by management to address the risks. Internal control does not encompass ensuring that the optimal risk response is chosen. For instance, the management of one company may choose to share technology risk by outsourcing certain aspects of its technology processing with a company experienced in that field, while another company may choose to retain its technology processing and develop general controls over technology activities for managing related technology risks. Neither of these choices should be viewed as right or wrong, as each 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.

251 Once management has chosen to reduce or share a risk, control activities can then be selected and developed. This is the focus of the following chapter. 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. 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.

252 Management may also need to review the level of risk in light of changes and makes 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.

Principle 8.

Assesses Fraud Risk

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

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

254 The actions being conducted as part of applying this principle link closely to the preceding principle (see Identifies and Analyzes Risks), whereby risks relating to the achievement of objectives are identified and assessed. That principle 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.

Fraudulent Reporting

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

256 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 automation.
- Unusual or complex transactions subject to significant management influence.
- Vulnerability to management override and potential schemes to circumvent existing control activities.

257 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 is not 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.

Safeguarding of Assets

258 Safeguarding of assets refers to protecting against the unauthorized and willful 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

259 Safeguarding of assets typically relates primarily 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 relate to the operations objectives but are not directly linked to safeguarding of assets.

260 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 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.

261 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.

262 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

263 In addition to assessing risks relating to the safeguarding of assets and fraudulent reporting, management considers possible corruption occurring within the entity. 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).

264 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.

Opportunity, Attitudes, and Rationalization

265 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

266 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

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

- A person labelling the use of resources as borrowing, and fully intending to pay the stolen money back at some point.

- A person, because of job dissatisfaction (salary, job environment, treatment by managers, etc.), believing that something is owed to him or her.
- A person being unable to understand or not caring about the consequence of his or her actions or of accepted notions of decency and trust.

Other Considerations in Fraud Risk Assessment

268 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 various 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 implement more extensive anti-fraud programs cost effectively.

269 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.

Principle 9.

Identifies and Analyzes Significant Change

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

270 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, formal or informal, to identify and assess those internal and external factors that can significantly affect its ability to achieve its objectives.

271 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 mechanisms in place to identify and communicate activities that affect the entity's objectives—and assessing 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.

272 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.

273 Mechanisms exist 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.

Circumstances Requiring Special Attention

274 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. Conditions may include:

- *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 such care facilities. Each of these changes may require the 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.
- *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 manage 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 to grow the business and/or reduce costs, but 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 these new environments 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.
- *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.

Summary of Principles and Attributes Relating to Risk Assessment

Noted below are the four principles and related nineteen attributes for Risk Assessment.

Specifies Relevant Objectives

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

The chart below depicts attributes that apply to each objective category. This chart reflects in summary form the six attributes relating to Principle 6. Each attribute is stated in detail below for each category of objective.

	Operations	Reporting			Compliance
		Internal	External Non-Financial	External Financial	
a. Considers Tolerance for Risk/ Required Level of Precision/ Materiality	✓	✓	✓	✓	✓
b. Complies with Externally Established Standards, and Frameworks/Complies with Applicable Accounting Standards /Reflects External Laws and Regulations			✓	✓	✓
c. Reflects Management's Choices	✓	✓			
d. Reflects Entity Activities		✓	✓	✓	
e. Includes Operations and Financial Performance Goals	✓				
f. Forms Basis for Committing of Resources	✓				

Attributes Relating to Operations Objectives

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

Attributes Relating to Reporting Objectives

For the reporting category of objectives, attributes noted are separate for internal reporting, external non-financial reporting, and external financial reporting.

External Financial Reporting

- **Considers Materiality**—Management considers materiality in financial statement presentation.
- **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.
- **Reflects Entity Activities**—External reporting reflects the underlying transactions and events within a range of acceptable limits.

External Non-financial Reporting Objectives

- **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.
- **Complies with Externally Established Standards and Frameworks**—Management establishes objectives consistent with standards and frameworks established by recognized external organizations.
- **Reflects Entity Activities**—External reporting reflects the underlying transactions and events within a range of acceptable limits.

Internal Reporting Objectives (financial and/or non-financial)

- **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 Management's Choices**—Internal reporting provides management with accurate and complete information regarding management's choices and information needed in managing the organization.
- **Reflects Entity Activities**—Internal reporting reflects the underlying transactions and events within a range of acceptable limits.

Attributes Relating to Compliance Objectives

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

Identifies and Analyzes Risks

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.*

- **Involves Appropriate Levels of Management**—The organization puts into place effective risk assessment mechanisms that involve appropriate levels of management.
- **Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels**—The organization identifies and assesses risks at the entity, subsidiaries, 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.
- **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.

Assesses Fraud Risk

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

- **Considers Various Ways That Fraud Can Occur**—The assessment of fraud considers possible loss of assets, fraudulent reporting, and corruption resulting from the various ways that fraud and misconduct can occur.
- **Considers Risk Factors**—An entity's assessment considers factors that influence the significance of the loss of assets and the related impact on operations, reporting, and compliance activities.
- **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.

Identifies and Analyzes Significant Change

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

   - **Assesses Changes in the External Environment**—The risk identification process considers changes to external factors that can significantly affect the entity's ability to achieve objectives.
   - **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, changing reliance on foreign geographies, new technologies, and changes to the physical environment in which the business operates.
   - **Assesses Changes in Leadership**—The organization considers changes in management and their respective attitudes and philosophies on the system of internal control.

Control Activities

Chapter Summary:

275 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:

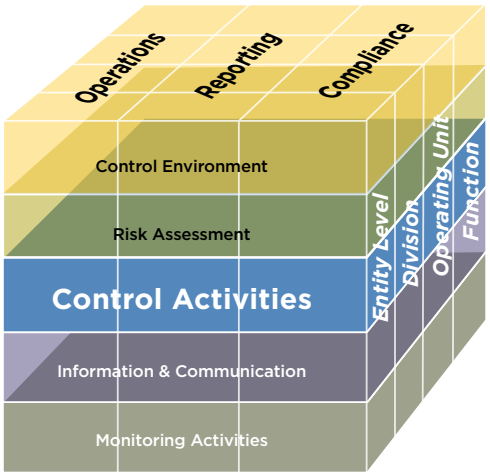
10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

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

12. The organization deploys control activities as manifested in policies that establish what is expected and in relevant procedures to effect the policies.

Introduction

276 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.



277 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 necessary to support the reporting compliance and operations objectives.

Principle 10.

Selects and Develops Control Activities

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

Integration with Risk Assessment

278 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.

279 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.

280 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

281 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.

282 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

283 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.[14] 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."[15]

284 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.

285 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 process risks into a more manageable form is to group them according to information-processing objectives[16] of completeness, accuracy, and validity. 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.

286 The following information-processing objective definitions are used in this *Framework*:

- *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.
- *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).

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

15 The term "transaction controls" is used in this *Framework* to refer to both manual and automated controls.

16 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.

- *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 (i.e., approval by a person having the authority to do so) of transactions as specified by an organization's established policies and procedures. In an operational context, the parts used in making an automobile are obtained from an authorized supplier.

287 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 may also be considered 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.

288 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 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).

289 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.

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

Types of Transaction Control Activities

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

- *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.

- *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.
- *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.
- *Physical Controls*—Equipment, inventories, securities, cash, and other assets are secured physically (i.e., 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.
- *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 judgmentally selects and develops supervisory controls over higher risk transactions. For instance, a supervisor may review[17] 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).

292 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.

17 Supervisory reviews can be either control activities or monitoring activities. The difference is discussed further in Chapter 7, Monitoring Activities.

293 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, 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).

294 When selecting and developing control activities it is important to understand what a particular control is designed to accomplish (i.e., what specific risk response does the control address) and how well it does it (in terms of efficiency and effectiveness). For example, 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. 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

295 Control activities and technology[18] 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. In this *Framework*, these procedures are known as automated control activities or automated controls. Automated controls include financial process-related automated transaction controls, such as a three-way match performed within an enterprise resource planning (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

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

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.

296 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.

297 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

298 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 usually are business performance or analytical reviews 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.

299 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.

300 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.

301 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 will tend to be greater the higher the levels in the organization that business performance reviews are applied. 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.

302 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

303 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 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 and enable it to 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.

304 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, including management override. 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.

305 However, sometimes segregation is not practical 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[19] control activities. Using 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.

19 This *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 this *Framework*.

Principle 11.

Selects and Develops General Controls over Technology

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

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

306 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.[20] 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.

307 Technology general controls must be implemented and operating 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 initially developed and 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 intended.

308 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. Control activities are selected and developed that contribute to the mitigation of specific risks surrounding the use of technology processes.

20 Terminology in existing literature varies. These controls are sometimes called "general computer controls," "general controls," or "information technology controls." The term "technology general controls" is used here for convenience to refer to "general control activities over technology."

Technology General Controls

309 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, 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.

Technology Infrastructure

310 Technology requires an infrastructure in which to operate, ranging from communication networks for linking technologies to each another 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.

311 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

312 Security management includes sub-processes and control activities over who and what has access to an entity's technology. They generally cover access rights at the data, operating system (system software), network, application, and physical layers. Security controls over the access to an entity's technology protects it from inappropriate access and unauthorized use of the system. 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).

313 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 within their business and business processes. 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.

314 Internal threats from former or disgruntled employees 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 due to greater access and knowledge of the entity's security management systems and processes.

315 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 where authorized users are restricted to the applications or functions commensurate with their job responsibilities and support 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

316 Technology general controls support the acquisition, development, and maintenance of technology. For example, a technology development methodology[21] provides a structure for system design and implementation, outlining specific phases, documentation requirements, approvals, and checkpoints to control 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.

317 In some companies the development methodology covers the continuum from large development projects to the smallest changes. In other companies there is a distinct process and methodology 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.

318 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.

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

319 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 the selection and implementation.

320 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.

Principle 12.

Deploys through Policies and Procedures

The organization deploys control activities as manifested in policies that establish what is expected and in relevant procedures to effect the policies.

321 An entity deploys many policies and procedures to achieve its objectives. 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.

322 Many times policies and procedures are 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. But whether or not it is written, a policy must establish clear individual responsibility and accountability and be deployed thoughtfully and conscientiously, and the related procedures must be timely and be performed diligently and consistently by competent personnel. A procedure will not be useful if performed by rote, without a sharp, continuing focus on the risks to which the policy is directed.

323 Further, it is essential that questionable matters identified as a result of the procedure be investigated and, if appropriate, corrective actions be taken in a timely manner. For example, suppose 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 recorded properly. The receipt is reapplied and the correction is reflected in the reconciliation.

324 Follow-up actions vary depending on the size and structure of the entity. They could range from formal internal communication processes in a large company where operating units state why performance targets were not met and what actions are being taken to prevent a recurrence to an owner-manager of a small business walking down the hall to speak with the plant manager about what went wrong and what needs to be done.

325 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. For example, management may upgrade the purchasing module of an enterprise resource planning (ERP) system and introduce new automated transaction control activities that cause the old manual control activities to be redundant and hence no longer necessary.

Summary of Principles and Attributes Relating to Control Activities

Noted below are the three principles and related sixteen attributes for Control Activities.

Selects and Develops 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.

- **Integrates with Risk Assessment**—Control activities help ensure that risk responses that address and mitigate risks are carried out.
- **Determines Relevant Business Processes**—Management determines which relevant business processes require control activities.
- **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.
- **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.

Selects and Develops General Controls over Technology

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

- **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.

Deploys through Policies and Procedures

12. *The organization deploys control activities as manifested in policies that establish what is expected and in relevant procedures to effect the policies*

- **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 Using Competent Personnel**—Competent personnel perform control activities with diligence and continuing focus.
- **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.
- **Reassesses Policies and Procedures**—Management periodically reviews control activities to determine their continued relevance, and refreshes them when necessary.

Information and Communication

Chapter Summary:

326 Information is necessary for the entity to carry out internal control responsibilities in support of 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:

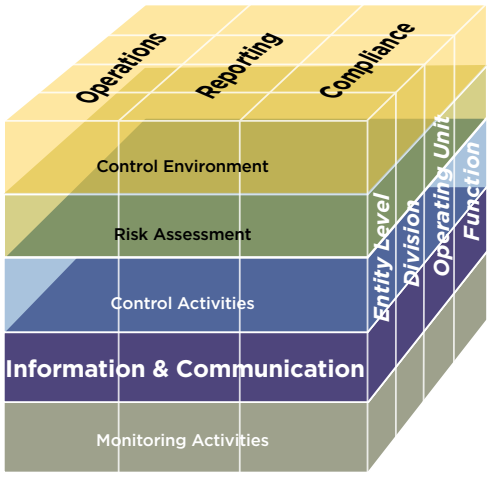
13. The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.

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

327 The Information and Communication component of the *Framework* supports the functioning of other components of internal control. In combination with the other components, information and communication support the achievement of the entity's objectives, including objectives relevant to internal and external reporting. Users of the *Framework* should differentiate reporting objectives from the information and communication component in establishing the system of internal control.



328 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 by processing relevant, timely, and quality information from internal and external sources.

329 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.

Principle 13.

Uses Relevant Information

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

330 Information is necessary for the organization to carry out their internal control responsibilities in support of 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. 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, a balanced scorecard that mapped these goals to metrics and to actual results, both non-financial and financial, was provided every month basis. Feedback from a subsequent employee survey indicated that management and other personnel better understood the organization's objectives.

Information Requirements

331 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.

332 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 up-time 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.

333 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

334 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.

Information from Relevant Sources

335 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
1 Email communications	• Organizational changes
2 Inspections of production floor processing	• On-time and quality production experience
3 Minutes or notes from operating committee meetings	• Actions in response to energy consumption metrics
4 Personal time reporting system	• Hours incurred on time-based projects
5 Reports from manufacturing systems	• Number of units shipped in a month
6 Responses to customer surveys	• Factors impacting customer attrition rates
7 Whistle-blower hotline	• Complaint on manager's behavior

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

336 Management considers a comprehensive scope of potential events, activities, and data sources, available internally and from reliable external sources, and selects those that are 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 the nature, extent, and sources of information and underlying data to meet its ongoing needs.

Processing Data through Information Systems

337 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, and technology that support business processes managed internally as well as those that are supported through relationships with outsourced service providers and other external parties.

338 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.

339 The volume of information accessible to the organization presents both opportunities and risks. Greater access to information can enhance internal control.

340 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, or 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.

341 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.

342 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.

343 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.

344 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 Quality

345 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.

346 The quality of information depends on whether it is:

- *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.
- *Current*—The data gathered is from current sources and is gathered at the frequency needed.
- *Correct*—The underlying data is accurate and complete. Information systems include validation checks that address accuracy and completeness, including necessary exception resolution procedures.
- *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.
- *Protected*—Access to sensitive information is restricted to authorized personnel. Data categorization (e.g., confidential and top secret) supports information protection.
- *Verifiable*—Information is supported by evidence from the source.
- *Retained*—Information is available over an extended period of time to support inquiries and inspections by external parties.

347 Management establishes information management policies with clear responsibility and accountability for the quality of the information. For example, 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.

348 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 including information quality. Information requirements are developed by the organization and communicated to outside service providers and other similar external parties. Control activities are defined to 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.

Principle 14.

Communicates Internally

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

349 Communication of information conveyed across the entity includes:

- The importance, relevance, and benefits of effective internal control.
- The roles and responsibilities of management and other personnel in performing controls.
- The 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.

350 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 Control Communication

351 Internal communication begins with the communication of 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.

352 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.

353 In addition, information that is shared through internal communication helps management and other personnel recognize any problems or potential problems, determine their cause, and take corrective action. For example, the 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. This information 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.

354 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.

355 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 such as whether the code of conduct is understood and adhered to, competence of personnel, potential management override of controls, or issues that employees may not otherwise feel comfortable sharing. Additionally, the overall system

of internal control is enhanced by the existence of an 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

356 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 or interest to deal with problems they have uncovered. Compounding the problem is that an unreceptive manager is usually the last to know that the normal communications channel is inoperative or ineffective.

357 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 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.

358 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 upon information that is reported to them.

Method of Communication

359 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.

360 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 discussion
- Performance evaluations
- Policies and procedures
- Presentations
- Social media postings
- Text messages
- Webcast and other video forms
- Website or collaboration site postings

361 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 (e.g., code of conduct, anti-money laundering, and corporate security) should be retained.
- 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).

362 Regardless of the method of communication used, management considers its requirements to retain communications, particularly those to 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. Control activities over retention of internal control information consider the challenges of advances in technology, including communication and collaboration technologies used to support internal control.

363 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.

Principle 15.

Communicates Externally

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

364 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, business partners, owners, customers, regulators, financial analysts, and other external parties.

365 The organization establishes and implements policies and procedures that facilitate effective external communication. This includes mechanisms 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.

Outbound Communication

366 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 is critical to establishing the 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 distributes its policies and practices for 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.

Inbound Communication

367 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, 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.

368 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 over (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.

369 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 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 external parties 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

370 Complexity of business relationships between the entity and external reviewers 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 external parties, such as customers, suppliers, and external 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

371 Similar to internal communications, the means by which management communicates externally impacts 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 company information through a customer portal may receive messages through postings made on their website.

372 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.

Summary of Principles and Attributes Relating to Information and Communication

Noted below are the three principles and related fourteen attributes for Information and Communication.

Uses Relevant Information

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

- **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 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.

Communicates Internally

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

- **Communicates Internal Control Information with Personnel**—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.

Communicates Externally

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

- **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.
- **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.
- **Communicates with the Board of Directors**—Relevant information resulting from assessments conducted by external parties is communicated to the board of directors.
- **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.

Monitoring Activities

Chapter Summary:

373 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. 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 management's criteria and deficiencies are communicated to management and the board of directors as appropriate.

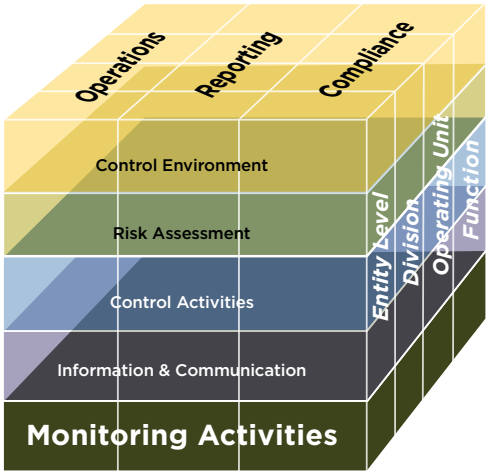
Principles relating to the Monitoring Activities Component:

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

374 Monitoring activities assess whether each of the five components of internal control are present and functioning. The organization uses ongoing and separate evaluations to ascertain whether 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.



375 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 able to address new risks.

376 Where appropriate, monitoring activities identify and examine expectation gaps relating to anomalies and abnormalities, which may indicate that one or more components of internal control, including controls to effect principles across the entity and its subunits, are not present and functioning. Monitoring activities will generally identify root causes of such breakdowns. Monitoring activities operate within various business processes and across the entity and its subunits.

377 Organizations need to consider underlying details in determining whether an activity is a control activity versus a monitoring activity especially where the activity involves some level of supervisory review. Review activities are not automatically classified as monitoring activities. 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 task management with 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.

378 The following examples 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.	• Semi-annually, management evaluates whether supervisors performing the review and approval are properly trained and knowledgeable.

Principle 16.

Conducts Ongoing and/or Separate Evaluations

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

379 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 usually are 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.

380 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. An entity that perceives a need for frequent separate evaluations may consider identifying ways to enhance ongoing evaluations.

381 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 implemented and are operating as intended. The decision of whether to conduct ongoing, 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.

382 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.

383 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.

384 Understanding the design and current state of a system of internal control system provides useful baseline information for establishing ongoing and separate evaluations. When change occurs within the components of internal control the baseline may need to be re-evaluated to make sure monitoring activities are aligned with the other components of internal control.

Ongoing Evaluations

385 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.

386 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 continuing monitoring computer applications available, and these should be considered when selecting ongoing evaluations.

387 The following examples illustrate ongoing evaluations.

The quality officer of a medium-size manufacturing company participates in a monthly production meeting where he or 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 or her 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

388 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 present and functioning. 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. 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.

389 Separate evaluations are often conducted through the internal audit function and while having an internal audit function is not a requisite of internal control[22], it can enhance the scope, frequency, and objectivity of such reviews. Since separate evaluations are conducted periodically by independent managers, employees, or external parties to provide feedback with greater objectivity, evaluators need to be knowledgeable about

22 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 this exchange to have an internal audit function (NYSE Listed Company Manual 303A.07(d)).

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.

390 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.

Separate Evaluation Approaches

391 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, the internal audit function develops each year 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 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 entities 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 specialist, IT security specialists, consultants, or others in considering the presence and functioning of components of internal control. For example, an entity's IT security specialist periodically evaluates 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 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, 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, the chief executive of a food product division directs the evaluation of its internal control activities related to food safety regulations. He or 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

392 Entities that use outsourced service providers for services such as third-party warehousing, internet hosting, health care 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.

393 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.[23] When reviewing such reports, organizations should 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. 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.

23 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).

Principle 17.

Evaluates and Communicates Deficiencies

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.

394 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 the 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.

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

- 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 that 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.

Communication of Findings

396 Results of ongoing and separate evaluations are assessed against management's criteria to determine to whom to report and what is reported.

397 All identified internal control deficiencies that can affect an entity's ability to develop and achieve its objectives are communicated to those positioned to take timely corrective actions. Additionally scope and approach, as well as any deficiencies, may need to be reported to those conducting the overall assessment of effectiveness of internal control and concluding thereon.

398 The nature of matters to be communicated varies depending on how the deficiency is evaluated against management's criteria, individuals' authority to deal with circumstances that arise, and the oversight activities of superiors. After deficiencies are evaluated management tracks whether remediation efforts are conducted on a timely basis.

399 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. 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 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.

400 In considering what needs to be communicated, it is necessary to look at the implications of findings. 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.

Reporting to Senior Management and the Board of Directors

401 Providing information on internal control deficiencies to the right party is critical. Deficiencies that are categorized as material weaknesses, significant deficiencies, minor non-conformities, and major non-conformities are reported to senior management and the board of directors, as appropriate and in accordance with the reporting directives that the entity has established. For example, the board of directors may ask management or internal or external auditors to communicate material weaknesses, significant deficiencies, major non-conformities and other deficiencies and nonconformities that meet a specified threshold.

402 Additionally, deficiencies may need to be reported externally. This depends on the type of entity and the requirements they are subject to.

Summary of Principles and Attributes Relating to Monitoring Activities

Noted below are the two principles and eleven related attributes for Monitoring Activities.

Conducts Ongoing and/or Separate Evaluations

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

- **Considers a Mix of Ongoing and Separate Evaluations**—Management includes a balance of 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.
- **Considers Rate of Change**—Management considers the rate of change in business and business processes when selecting and developing 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.
- **Objectively Evaluates**—Separate evaluations are performed periodically to provide objective feedback.
- **Adjusts Scope and Frequency**—Management varies the scope and frequency of separate evaluations depending on risk.

Evaluates and Communicates Deficiencies

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.*

- **Assesses Results**—Management and the board of directors, as appropriate, assess results of ongoing and separate evaluations.
- **Communicates Deficiencies to Management**—Deficiencies are communicated to parties responsible for taking corrective action and to at least one level of management above.
- **Reports Deficiencies to Senior Management and the Board of Directors**—Deficiencies are reported to senior management and to the board of directors, as appropriate.
- **Monitors Corrective Actions**—Management tracks whether deficiencies are remediated on a timely basis.

Limitations of Internal Control

Chapter Summary:

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

404 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.

405 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 related to the effectiveness and efficiency of an entity's operations—achieving its basic mission, profitability goals, and the like—internal control can help to ensure that management is aware of the entity's progress, or lack of it. But it cannot provide even reasonable assurance that the objectives themselves will be achieved.
- Second, internal control cannot provide absolute assurance for any of the three objectives categories.

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

407 Reasonable assurance certainly does not imply that internal control systems will frequently fail. Many factors, individually and collectively, serve to strengthen the concept of reasonable assurance. The cumulative effect of controls that satisfy multiple objectives and the multipurpose nature of 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, among a cross-section of well-controlled entities, it is very likely that most will be regularly apprised of movement toward their operations objectives, will regularly achieve compliance objectives, and will consistently produce—period after period, year after year—reliable external reporting. However, because of the inherent limitations discussed above, there is no guarantee that, for example, an uncontrollable event, mistake, or improper reporting incident could never occur. In other words, even an effective internal control system can experience a failure. Reasonable assurance is not absolute assurance.

Preconditions of Internal Control

408 This *Framework* specifies several areas that are part of the management process but not part of internal control. Two such areas relate to objectives being 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 key 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, an entity that has an ineffective strategy-setting and objective-setting process may be challenged in its ability to achieve poorly constructed, unrealistic, or unsuitable objectives. The internal control process cannot encompass all activities undertaken by the entity, and weaknesses in these important areas may impede the organization in having effective internal control.

Judgment

409 The effectiveness of controls 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

410 Even if internal controls are well designed, they can break down. Personnel may misunderstand instructions, they may make mistakes in judgment, or they may commit errors due to carelessness, distraction, or being asked to focus on too many tasks. For example, an accounting 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 carrying out control duties for vacationing or sick employees might not perform correctly. System changes may be implemented before personnel have been trained to react appropriately to signs of incorrect functioning.

Management Override

411 An internal control system can only be as effective as the people who are responsible for its functioning. Even an entity with an effective system of internal control may have a manager who is willing and able to override internal control.

412 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 financial condition or compliance status. A manager of a division or operating unit, or a member of senior management, might override the control for many reasons: to increase reported revenue to cover an unanticipated decrease in market share, to enhance reported earnings to meet unrealistic budgets, to boost the market value of the entity prior to a public offering or sale, to meet sales or earnings projections to bolster bonus payouts tied to performance, to appear to cover violations of debt covenant agreements, or to hide lack of compliance with legal requirements. Override practices include deliberate misrepresentations to bankers, lawyers, accountants and vendors, and intentionally issuing false documents such as purchase orders and sales invoices.

413 Management override should not be confused with management intervention; the latter refers to management’s actions to depart from prescribed policies or procedures for legitimate purposes. Management intervention is necessary to deal with non-recurring and non-standard transactions or events that otherwise might be handled inappropriately by the control system. Providing for management intervention is necessary in all internal control systems because no system can be designed to anticipate every condition. Management’s actions to intervene are generally overt and commonly documented or otherwise disclosed to appropriate personnel, whereas actions to override usually are not documented or disclosed, and there is intent to cover up the actions.

Collusion

414 Collusion can result in control failures. Individuals acting collectively to perpetrate and conceal an action from detection often can alter financial data or other management information so that it cannot be identified by the control system. Collusion can occur, for example, between an employee who performs an important control function and a customer, supplier, or another employee may occur. On a different level, several layers of sales or operating unit management might collude in circumventing controls so that reported results meet budgets or incentive targets.

Roles and Responsibilities

Chapter Summary:

415 Everyone in an organization has responsibility for internal control. The board of directors or equivalent oversight body guides and directs management in the development and performance of internal control. Management is responsible for the establishment and performance of the entity's internal control system, with the chief executive officer, supported by senior management, being ultimately responsible and supported by senior management. Various business-enabling functions communicate, enable, and evaluate adherence to requirements defined by external laws, regulations, standards, internal policies and standards of conduct. Internal auditors evaluate and recommend improvements for the effectiveness of internal control, but they do not have any primary responsibility for establishing or maintaining it. While external auditors and reviewers are not responsible for the effectiveness of the internal control system, they provide another independent view on the reliability of the entity's external reporting. Likewise, other external parties, such as outsourced service providers, may be delegated tasks to sustain and promote internal control, but the responsibility for internal control remains with the delegating management.

Introduction

416 Internal control is effected by personnel internal to the organization, including management and the board of directors, business-enabling functions, and internal auditors. Collectively, they contribute to providing reasonable assurance that specified objectives are achieved.

417 Roles are sometimes described as being in one of three lines of defense to support the achievement of objectives:

- 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 consideration and implementation; their position and compensation are separate and distinct from the business areas they review.

418 Parties external to the organization such as outsourced service providers may also help with the achievement of objectives by providing information useful to exercising management control. The entity may audit their adherence to contractual obligations and imposed standards of conduct and control. However, external parties are not responsible for the entity's system of internal control.

Responsible Parties

419 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

420 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 this *Framework*, these governance structures are commonly referred to as the board of directors.

421 Management is accountable to the board of directors. With the power to engage or terminate management, the board has a key role in defining expectations on integrity and ethical values and 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 have an open and unrestricted communications channel with all entity personnel, the internal auditors, independent auditors, external reviewers, and legal counsel.

422 Boards of directors usually carry out certain duties through committees. Their use varies depending on regulatory requirements and other considerations. Board committees may be used for oversight of audit, compensation, nominations and governance, 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.

423 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. The audit committee, along with a strong internal audit function, is often best positioned, as a result of its independence, to identify and promptly act in situations where senior management overrides controls or deviates from expected standards of conduct. While board composition requirements vary, independent directors are important as they can provide an objective perspective. For example, the New York Stock Exchange and the National Association of Securities Dealers in the US require audit committees to have a majority of independent directors. Besides independence, audit committees are required to demonstrate certain skills and competencies, notably financial reporting expertise, internal control over financial reporting, and familiarity with information technology use.
- *Compensation Committee*—This committee provides oversight of compensation arrangements and aligns pay with performance. It seeks to motivate senior management without providing incentives for undue risk-taking to ultimately protect and promote the interest of shareholders or other owners of the entity. It oversees 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*—This 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. 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

424 The chief executive officer (CEO) is ultimately responsible for the effectiveness of the entity's internal control system. More than any other individual or function, the CEO sets the tone at the top that affects control environment factors and all other components of internal control.

425 The CEO fulfills this duty by:

- Providing leadership and direction to senior management. With the support of management, the CEO shapes the values, principles, and major operating policies that form the foundation of the entity's internal control system. For example, the CEO and senior management set entity-wide objectives and broad-based policies. They take actions concerning the entity's organizational structure, content, and communication of key policies, and the type of planning and reporting systems the entity will use.
- Meeting periodically with senior management from each of the operating units (e.g., research and development, production, marketing, sales) and major business enabling functions (e.g., finance, human resources, legal, compliance, risk management).
- Defining metrics, targets, or other measurable expectations with which to gauge the ongoing and long-term effectiveness of the system of internal control. The methods of designing, implementing, and assessing internal control are delegated to management at different levels.

- Directing all management and other personnel to proactively identify threats to the system of internal control. Given the ever-increasing pace of change and networked interactions of business partners, customers, and employees, the sources of threat to an ongoing effective internal control system are constantly changing. The CEO expects senior management in particular to beware of making assumptions based on the traditional sources of threats to an effective internal control system.

426 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

427 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 established, risks are analyzed, and decisions are made on how changes will be managed.

428 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.

429 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

430 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 operating officer
- Chief administrative officer
- Chief risk officer
- Chief compliance officer
- Chief information officer
- Other senior leadership roles, depending on the nature of the business

431 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.

432 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 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.

433 Depending on the number of layers of management, 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 backorders or product inventory positions. Issues are communicated up the organization's reporting structure according to the level of severity associated with the issue. 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.

434 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 owners of the entity.

Business-Enabling Functions

435 Various functions support the business through their 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 also 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.

436 While each control function serves 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

437 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.

438 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. 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

439 Counsel from legal professionals is key to defining effective controls for compliance with regulations and managing the possibility of lawsuits. For large and complex organizations, specialized compliance professionals can be helpful to defining and assessing controls for adherence to both external and internal requirements.

440 A close working relationship between business management and legal and compliance personnel provides a strong basis for designing, implementing, and assessing appropriate 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

441 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. 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.
- *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 information used in the internal control system (e.g., inventory records, work-in-process data, sales or expense reports) or take other actions needed to effect control.

- *Monitoring Activities*—Support 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.

442 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

443 As the third line of defense, internal auditors provide assurance and advisory services over 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. The size of the internal audit function depends on the size, complexity, and geographic expanse of the overall entity and its sub units. In all cases, internal audit activities are expected to be carried out by competent and professional resources aligned to the risk relevant to the entity.

444 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:

- 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.

445 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.

446 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.

447 Internal auditors maintain an impartial view of the activities they audit through their position, 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.

448 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

449 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

450 Many organizations outsource business functions, delegating their specified roles and responsibilities for day-to-day management to outside service providers or other external parties. Administrative, finance, human resources, legal, and even select internal operations can be executed by parties outside the organization, with the objective of obtaining access to enhanced capabilities and lower cost of services. 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.

Business Partners and Other Parties Interacting with the Entity

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

- A customer, for example, 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.

452 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.

453 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

454 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.

455 In some jurisdictions, the auditor is also engaged or required by law or regulation 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.

456 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

457 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

458 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.

459 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

460 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.

461 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.

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**—Controls 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, general partners for a partnership, or owner for a small business.
- **Category**—One of three groupings of objectives of internal control. The categories are effectiveness and efficiency of operations, reliability of reporting, and compliance with applicable laws and regulations.
- **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, used as a subject (e.g., existence of a control), a policy or procedure that is part of internal control. Controls exist within each of the five components. **(2)** A noun, used as an object (e.g., to effect control), the result of policies and procedures designed to control; this result may or may not be effective internal control. **(3)** A verb (e.g., to control), to establish, or implement a policy that effects control.
- **Control Activity**—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.
- **Criteria**—A set of standards against which an internal control system can be measured in determining effectiveness.
- **Deficiency**—A 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.
- **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 in the following categories:
  - Effectiveness and efficiency of operations
  - Reliability of reporting
  - Compliance with applicable laws and regulations
- **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's statement of what should be done to effect control. A policy serves as the basis for procedures.
- **Present and Functioning**—Applied to components, principles, and attributes. Present means that a component, principle, or attribute has been implemented. Functioning means that a component, principle, or attribute is operating as intended.
- **Preventive Control**—A control designed to avoid an unintended event or result (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 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.
- **Reporting**—Used with "objectives" or "controls": having to do with the reliability of reporting.
- **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**—Includes 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.
- **System of Internal Control**—A synonym for Internal Control.
- **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. Summary of Changes to the 1992 Version of the Internal Control—Integrated Framework

462 This Appendix summarizes both the broad changes relevant across the entirety of the 1992 *Framework* as well as the changes made within each of the five components of internal control. The following are the more significant changes across all areas of the *Framework*:

- **Applies a principles-based approach**—The updated *Framework* focuses greater attention on principles. While the 1992 version 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 attributes, representing characteristics associated with the principles. Together, the principles and attributes comprise the criteria that will assist management in assessing whether an entity has effective internal control.
- **Clarifies the role of objective-setting in internal control**—The 1992 *Framework* stated that objective-setting was a management process, and that having objectives was a pre-condition to internal control. The updated *Framework* preserves that view, but moves the primary discussion to the Overview chapter from the chapter on risk assessment to emphasize the point that objective-setting is not part of internal control.
- **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 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.
- **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.

- **Enhances consideration of anti-fraud expectations**—The 1992 version considered fraud, although the discussion of anti-fraud expectations and the relationship between fraud and internal control was less prominent. This 2012 version contains considerably more discussion on fraud and also considers the potential for fraud as a principle of internal control.
- **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 further encompass the use of external parties for providing 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.

463 This reliance on external parties has changed the entire value chain and the channels through which value is delivered. Organizations may apply this approach through a shared service business model, outsourcing to an external party, spinoff or joint venture, or other approach. Whatever approach is taken, the concept of a virtual organization—an organization that includes activities managed both internally and externally—is an attribute of nearly every business enterprise.

464 This 2012 *Framework* explicitly considers the extended business model including the responsibilities for internal control in this model and the achievement of effective internal control.

Overall *Framework* Layout

465 The 1992 *Internal Control—Integrated Framework* contains a chapter that presents the definition of internal control, the components of internal control, the relationship of objectives and components, and effectiveness. The 2012 version of the *Framework* presents these topics in two chapters: the first, Definition of Internal Control, defines internal control; the second, Overview of Internal Control, includes the remaining discussion on components of internal control, the relationship of objectives and components, and effectiveness. In addition, the chapter entitled Overview of Internal Control introduces the seventeen principles of internal control, discusses cost versus benefits of internal control, the changing role of technology, documentation, application of internal control in larger versus smaller entities, and deficiency considerations.

Key Changes to Internal Control Components

Control Environment

466 In the two decades since the publication of the *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 multi dimensional approach to governance and control and ability to report accordingly. There is an increased need for transparency as to how the organization operates and governs itself; reporting 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.

467 In the revised Control Environment chapter, 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.
- Providing more explicit discussion on what is involved in achieving the control environment.
- 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 organization structure with the Roles and Responsibility chapter so that major roles are used consistently across within the *Framework*.

Risk Assessment

468 Since 1992, the focus 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 1992 *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.

469 Users also noted that almost half of the 1992 Risk Assessment chapter focused on objectives, and that this focus was not needed if objective-setting was truly a precondition 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.

470 Within the Risk Assessment chapter, key changes therefore include:

- Repositioning to the Overview chapter much of the discussion on objective-setting, which continues to be viewed as a pre-condition to risk assessment. Discussions on categories of objectives, linkage between objectives, and achievement of objectives are no longer included within the Risk Assessment component. The Risk Assessment component focuses on articulating objectives relating to operations, reporting, and compliance with sufficient clarity so that any risks to those objectives can be identified and assessed.
- 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.
- 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

471 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 the 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 include myriad decentralized, mobile, intelligent and web-enabled technologies, which are increasingly located at a third-party service organization or on the "cloud." Also, the recent focus on improving controls in organizations, which has been promoted by the marketplace and regulation, has led to a deeper understanding of how control activities are effectively designed and implemented.

472 Therefore, within the Control Activities chapter, 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. The details on automated control activities and general controls over technology have been separated into discrete sections to clarify the distinction between the two.
- Expanding the discussion that control activities constitute a range and mix of various types of control techniques while providing a more detailed description of these types and techniques, and a way to categorize them. Also, transaction level controls are now clearly made distinct from controls at other levels of the organization. A more detailed discussion on information-processing objectives has been added.
- 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

473 The source, volume, and form of information and communication have expanded dramatically since 1992. Information sources have grown more diverse and complex, spanning external parties that support all or part of an organization's business processes (e.g., outsourcing service providers, joint ventures, and other arrangements that extend activities to parties outside the boundaries under the direct control of the organization) and internal and external networks designed to create unstructured information-sharing mechanisms (social media).

474 The volume of information, particularly information 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.

475 Within the Information and Communication chapter, key changes include:

- Emphasizing the 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 other third parties, emphasizing the importance of considering how processes may occur outside the company (e.g., by the use of third-party service providers that manage processes such as payroll, customer relationship management, data center operations, supply chain, manufacturing, etc.) and how the entity needs to obtain information from and communicate with parties that operate outside its legal and operational boundaries.

Monitoring Activities

476 In applying the 1992 version of the *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.

477 The changes to the principles in this 2012 *Framework* will not substantially alter the approaches developed for COSO's Guidance on Monitoring Internal Control Systems.

478 Within the chapter 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.

Roles and Responsibilities

479 In addition to the update of the five components of internal control, the discussion on roles and responsibilities has been updated. Within the Roles and Responsibilities chapter, key changes include:

- Adding a discussion of the responsibility of chief executive officer and chief financial officer to formally attest to the effectiveness of internal control in certain jurisdictions.
- Expanding the discussion of the type of committees at the board level and their underlying rationale.
- Adding external reviewers, alongside independent auditors, to reflect the different types of internal control reviews that can be performed of the entity.
- Updating the section on legislators and regulators with current illustrative discussions.
- Adding a section on outsourced service providers.
- Aligning roles and responsibilities defined in the section on organization structure section of the control environment.

C. Methodology

Background

480 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* or ICIF). This initiative was expected to make the existing *Framework* and related evaluation tools more relevant in the increasingly complex business environment so that organizations worldwide could better design, implement, and assess internal control. As the original author of the *Framework*, PricewaterhouseCoopers conducted this project by bringing together in-depth understanding of the 1992 *Framework*, rationale for decisions made in creating the *Framework*, and senior resources providing fresh market perspectives.

481 The *Framework* has been widely accepted by organizations implementing and evaluating internal control related to operations, compliance, and financial reporting objectives, and more recently, 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 provide greater clarity and a more comprehensive and relevant conceptual guidance and practical examples.

Project Structure

482 The COSO Board formed an Advisory Council comprising representatives from industries, academia, government agencies, and non-profit organizations to provide input as the project progressed. In addition, the updated *Framework* is being exposed to the public to capture additional input. Such due process has helped the update adequately address current challenges for organizations in their internal control.

Approach

483 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 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 team developed the update, including principles and attributes. The update draft was reviewed by key users and stakeholder groups to solidify reactions and suggestions.

- *Preparation for Public Exposure*—The 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.
- *Finalization*—In this phase, the updated *Framework* was issued for public exposure for a 90-day comment period. Upon receipt of comments, the project team reviewed and analyzed all comments received, and identified any needed modifications. The team then finalized the *Framework* and provided the update to the COSO Board for review and acceptance.

484 Within each project phase and between phases, as one might expect, many different and sometimes contradictory opinions were expressed on fundamental issues. The project team, with COSO Board oversight, carefully considered merits of positions put forth, both individually and in the context of related issues, and embraced those that helped in the development of a relevant, logical, and internally consistent document.

D. Comparison with COSO Enterprise Risk Management—Integrated Framework

485 In 2004, the Committee of Sponsoring Organizations of the Treadway Commission 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.

486 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 in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and to manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

487 This appendix outlines the relationship between the *Internal Control Framework* and the *Enterprise Risk Management Framework*.

Enterprise Risk Management is Broader than Internal Control

488 Enterprise risk management is broader than internal control, expanding and elaborating on internal control and focusing more fully on risk. Internal control is an integral part of enterprise risk management. The *Enterprise Risk Management—Integrated Framework* remains in place for entities and others looking more broadly at enterprise risk management.

Categories of Objectives

489 This *Internal Control – Integrated Framework* specifies three categories of objectives: operations, reporting, and compliance. *Enterprise Risk Management* specifies three similar objectives categories. Both frameworks 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.

490 The *Enterprise Risk Management—Integrated Framework* adds a fourth category of objectives, strategic objectives, which operate at a higher level than the others. Strategic objectives 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.

491 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. Operating within risk tolerance provides management greater assurance that the entity remains within its risk appetite, which, in turn, provides a higher degree of 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

492 A concept not contemplated in the *Internal Control—Integrated Framework* is a portfolio view of risk. Enterprise risk management requires that in addition to focusing on risk in considering the achievement of entity objectives on an individual basis, it is necessary to consider composite risks from a portfolio perspective. Internal control does not require that the entity develop such a view.

Components

493 With the enhanced focus on risk, the *Enterprise Risk Management Framework* expands the internal control framework's risk assessment component, creating four components: objective-setting, event identification, risk assessment, and risk response.

494 In the *Enterprise Risk Management—Integrated Framework*, the objective setting component considers the process used by management and the board for setting strategic objectives and supporting objectives relating to operations, reporting, and compliance. Setting risk appetite and risk tolerance are key tenets of enterprise risk management. Internal control views the setting of objectives and risk tolerance as preconditions to an effective system of internal control.

495 Each of the five components of internal control are reviewed below in relation to the *Enterprise Risk Management—Integrated Framework.*

Control Environment

496 In discussing the Control Environment component, the *Enterprise Risk Management—Integrated Framework* discusses (in a 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.

497 Because of the critical importance of the board of directors and its composition, the *Enterprise Risk Management—Integrated Framework* expands on the *Internal Control—Integrated Framework*'s call for at least 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

498 The *Enterprise Risk Management—Integrated Framework* and the *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.

499 The *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 event, 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 is part of the broader strategy setting process.

500 While both frameworks call for assessment of risk, the *Enterprise Risk Management—Integrated Framework* suggests viewing risk assessment through a sharper lens. Risks are considered on an inherent and a residual basis, 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 and objectives and, where possible, observable data. The *Enterprise Risk Management—Integrated Framework* also calls attention to interrelated risks, describing how a single event may create multiple risks.

501 As noted, enterprise risk management encompasses the need for management to develop an entity-level portfolio view. With managers responsible for business unit, function, process, or other activities having developed a composite assessment of risk for individual units, entity-level management considers risk from a "portfolio" perspective.

502 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, where management considers 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

503 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 managing the entity.

Information and Communication

504 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 past periods under varying conditions. Current-state data provides important additional information, and data on potential future events and underlying factors completes the information 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

505 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.

E. Acknowledgments

506 The COSO Board and PwC gratefully acknowledge the efforts of the Advisory Council, including individuals, organizations, and accounting and consulting firms, regulatory observers, and other observers.

507 The COSO Board, Advisory Council, and PwC also acknowledge the many executives, legislators, regulators, auditors, academics, and others who gave their time and energy to participating in and contributing to various aspects of the study. Also recognized are the considerable efforts of the COSO organizations and their members who responded to surveys, participated in workshops and meetings, and provided comments and feedback throughout the development of this *Framework*.

508 Finally, COSO Board and PwC wish to acknowledge Dr. Larry Rittenberg, Ernst & Young, Professor of Accounting at the University of Wisconsin-Madison School of Business, and former COSO chair, who contributed greatly to this project. PwC also acknowledges the contribution of Richard M. Steinberg, a retired PwC partner and CEO of Steinberg Governance Advisors.

To submit comments on this Public Exposure Draft, please visit the **www.ic.coso.org** website. Responses are due by March 31, 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 the exposure draft will become part of the public record and will be available on-line until December 31, 2012.