5-2013

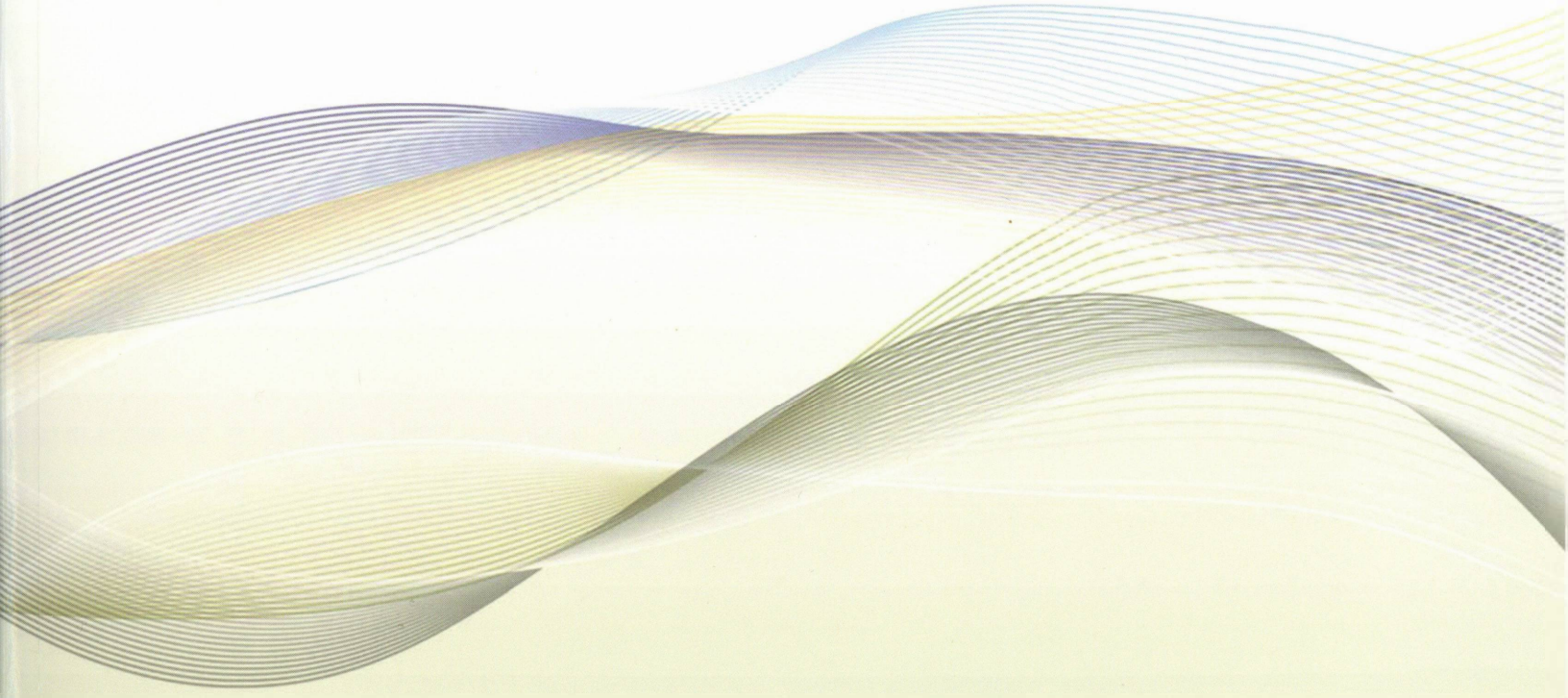
Internal Control — Integrated Framework Internal Control over External Financial Reporting: A Compendium of Approaches and Examples, May 2013

Committee of Sponsoring Organizations of the Treadway Commission

Committee of Sponsoring Organizations of the Treadway Commission

Internal Control — Integrated Framework

Internal Control over External Financial Reporting: A Compendium of Approaches and Examples



May 2013

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)

ISBN 978-1-93735-240-0

Committee of Sponsoring Organizations of the Treadway Commission

Internal Control — Integrated Framework

Internal Control over External Financial Reporting: A Compendium of Approaches and Examples

May 2013

Committee of Sponsoring Organizations of the Treadway Commission

Board Members

David L. Landsittel
COSO Chair

Mark S. Beasley
Douglas F. Prawitt
American Accounting Association

Richard F. Chambers
The Institute of Internal Auditors

Charles E. Landes
American Institute of Certified Public Accountants

Marie N. Hollein
Financial Executives International

Sandra Richtermeyer
Jeffrey C. Thomson
Institute of Management Accountants

PwC—Author

Principal Contributors

Miles E.A. Everson
Engagement Leader
New York, USA

Stephen E. Soske
Project Lead Partner
Boston, USA

J. Aaron Garcia
Project Lead Director
San Diego, USA

Cara M. Beston
Partner
San Jose, USA

Charles E. Harris
Partner
Florham Park, USA

Eric M. Bloesch
Managing Director
Philadelphia, USA

James M. Downs
Director
San Francisco, USA
(Through January 2012)

Catherine Jourdan
Director
Paris, France

Frank J. Martens
Director
Vancouver, Canada

Jay A. Posklensky
Director
Florham Park, USA

Charles J. Finn
Senior Manager
Detroit, USA

Natalie Protze
Senior Manager
Washington D.C., USA
(July 2011 to March 2012)

Sallie Jo Perraglia
Manager
New York, USA

Advisory Council

Sponsoring Organizations Representatives

Audrey A. Gramling
Bellarmine University
Fr. Raymond J. Treece Endowed Chair

Steven E. Jameson
Community Trust Bank
Executive Vice President and Chief Internal Audit & Risk Officer

J. Stephen McNally
Campbell Soup Company
Finance Director/Controller

Ray Purcell
Pfizer
Director of Financial Controls

William D. Schneider Sr.
AT&T
Director of Accounting

Members at Large

Jennifer Burns
Deloitte
Partner

James DeLoach
Protiviti
Managing Director

Trent Gazzaway
Grant Thornton
Partner

Cees Klumper
The Global Fund to Fight AIDS, Tuberculosis and Malaria
Chief Risk Officer

Thomas Montminy
PwC
Partner

Alan Paulus
Ernst & Young LLP
Partner

Thomas Ray
Baruch College

Dr. Larry E. Rittenberg
University of Wisconsin
Emeritus Professor of Accounting
Chair Emeritus COSO

Sharon Todd
KPMG
Partner

Kenneth L. Vander Wal
ISACA
International President 2011–2012

Regulatory Observers and Other Observers

James Dalkin
Government Accountability Office
Director in the Financial Management and Assurance Team

Harrison E. Greene Jr.
Federal Deposit Insurance Corporation
Assistant Chief Accountant

Christian Peo
Securities and Exchange Commission
Professional Accounting Fellow (Through June 2012)

Amy Steele
Securities and Exchange Commission
Associate Chief Accountant (Commencing July 2012)

Vincent Tophoff
International Federation of Accountants
Senior Technical Manager

Keith Wilson
Public Company Accounting Oversight Board
Deputy Chief Auditor

Additional PwC Contributors

Mark Cohen
Partner
San Francisco, USA

Andrew Dahle
Partner
Chicago, USA

Junya Hakoda
Partner (Retired)
Tokyo, Japan

Brian Kinman
Partner
St. Louis, USA

Pat McNamee
Partner
Florham Park, USA

Jonathan Mullins
Partner (Retired)
Dallas, USA

Alexander Young
Partner
Toronto, Canada

Antoine Elachkar
Managing Director
Washington D.C., USA

Frank Maggio
Director
Chicago, USA

Christopher Michaelson
Director
Minneapolis, USA

Tracy Walker
Director
Bangkok, Thailand

Qiao Pan
Senior Associate
New York, USA

Table of Contents

Foreword ..... **i**

1. Introduction 1
2. Control Environment 13
3. Risk Assessment 49
4. Control Activities 79
5. Information and Communication 111
6. Monitoring Activities 139

Appendices

A: Examples by Topic 156

B: Public Comment Letters 159

Foreword

In 2013, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) released an update to its *Internal Control—Integrated Framework* (*Framework*). The original framework, which was released in 1992, has gained broad acceptance and is widely used around the world. It is recognized as a leading framework for designing, implementing, and conducting internal control and for establishing requirements for an effective system of internal control. To help users apply the *Framework* to internal control over external financial reporting, COSO has released this companion publication, *Internal Control over External Financial Reporting: A Compendium of Approaches and Examples* (*Compendium*). More specifically, the *Compendium* provides approaches and examples to illustrate how entities may apply the principles set out in the *Framework* to a system of internal control over external financial reporting.

In the twenty years since the release of the original framework, business and operating environments have changed dramatically, becoming increasingly complex, technologically driven, and global. At the same time, stakeholders have become more engaged, seeking greater transparency and accountability for the integrity of systems of internal control that support business decisions and governance of the organization. The *Framework* and the *Compendium* incorporate many of these changes including:

- *Expectations for Governance Oversight*—Higher regulatory and stakeholder expectations require the board of directors to oversee internal control over external financial reporting. Some jurisdictions require specific regulatory requirements for expertise and independence of board members of certain types of entities.
- *Globalization of Markets and Operations*—Organizations expand beyond domestic markets in the pursuit of value, often entering into international markets and executing cross-border mergers and acquisitions.
- *Changes and Greater Complexities in the Business*—Organizations change business models and enter into complex transactions in pursuit of growth, greater quality, and productivity, and in response to changes in market and regulatory environments. These changes may include entering into strategic alliances, joint ventures, and other complex contractual arrangements with external parties, implementing shared services, and engaging outsourced service providers.
- *Demands and Complexities in Laws, Rules, Regulations, and Standards*—Regulators and policy makers promote greater investor protection and confidence in the financial reporting systems through changes in rules, regulations, and standards. Also, users of external financial reports seek greater amounts of information to better evaluate an entity's financial condition and operating results as businesses become more complex.
- *Expectations for Competencies and Accountabilities*—Demands for greater competence and accountability increase as organizations grow; acquire entities; introduce new products and services; comply with complex rules, regulations, and standards; and implement new processes and technologies. Organizations may flatten and shift management operating models and delegate greater authority or accountability to certain roles.

- *Uses of, and Reliance on, Evolving Technologies*—An increasingly mobile and interconnected world has made technology more essential for many organizations to improve performance, business processes, and decision making. Entities are investing in emerging technologies, such as cloud computing, mobile devices, and social media, and using enterprise resource planning (ERP) and other technologies to standardize, automate, and streamline business processes.
- *Expectations Relating to Preventing or Detecting Material Omissions and Misstatements and Fraud*—Stakeholders today have higher expectations for effective internal control over external financial reporting in preventing and detecting material omissions and misstatements due to error and fraud.

Each of these changes requires an organization to periodically evaluate the implications on its system of internal control over external financial reporting and to design and implement appropriate responses so that the system of internal control adapts and remains effective over time.

The *Compendium* provides practical approaches and examples that illustrate how the components and principles set forth in the *Framework* can be applied in preparing external financial statements. It neither replaces nor modifies the *Framework*; rather, it is a supplemental document that can be used in concert with the *Framework* when considering internal control over external financial reporting.

Finally, the COSO Board would like to thank PwC and the Advisory Council for their contributions in developing the *Compendium*. Their full consideration of input provided by many stakeholders and their attention to detail were instrumental in ensuring that the *Compendium* will be helpful to a variety of organizations in applying the *Framework* to internal control over external financial reporting.

David L. Landsittel
COSO Chair

1. Introduction

COSO's Internal Control—Integrated Framework (*Framework*) sets forth three categories of objectives: operations, reporting, and compliance. The focus of this publication, *Internal Control over External Financial Reporting: A Compendium of Approaches and Examples* (*Compendium*) is the external financial reporting category of objectives, a subset of the reporting category. External financial reporting objectives address the preparation of financial reports for external parties, including:

- Financial statements for external purposes
- Other external financial reporting derived from an entity's financial and accounting books and records

Using This Document

Intended Audience

The *Compendium* has been developed to assist those users of the *Framework* who are responsible for designing, implementing, and conducting a system of internal control over external financial reporting (ICEFR) that supports the preparation of financial statements and other external financial reporting. It is also relevant to entities that report on the effectiveness of a system of internal control over external financial reporting relating to the preparation of financial statements. The preparation of financial statements for external purposes and other external financial reporting applies to the following types of entities:

- *Public Entities*—Often, public entities are required to prepare financial statements for external purposes in accordance with applicable accounting standards, rules, and regulations. Additionally, they often prepare other external financial reporting derived from its financial and accounting books and records, such as earnings press releases, or information included in stipulated reports for business partners or lending agencies as required by contract.
- *Private Entities*—Entities whose ownership may be closely held may prepare financial statements to provide to banks and other third parties in order to raise capital or to meet contractual obligations. These statements can be prepared in accordance with standards and regulations, even though often, doing so may not be a requirement for private entities. More commonly, the form of the financial statements or of other external financial reporting is stipulated by contractual obligations or a third party.
- *Not-For-Profit Entities*—These entities may prepare financial statements for external purposes in accordance with appropriate rules and regulations. However, because the purpose of these entities is something other than realizing and generating profit, they may also prepare financial reporting for donors, government agencies, or other third parties that is not necessarily in accordance with specific standards, rules, or regulations, but aims to raise funds to support the stated cause.

- *Governmental Entities*—These entities prepare financial statements that are required by law. As well, they may prepare financial reporting in accordance with specific standards, rules, or regulations, but which is not necessarily required, for the public or governmental oversight agencies.

Approaches and Examples for Applying Principles

In applying the *Framework*, users will find relevant approaches and examples in the *Compendium* of how organizations may apply the principles in the design, implementation and conduct of internal control over external financial reporting. These approaches and examples relate to each of the five components and seventeen principles set forth in the *Framework*.

- *Approaches* describe how organizations may apply these principles within their system of internal control over external financial reporting. Approaches are designed to give users of the *Compendium* a summary-level description of activities that management may consider as they apply the *Framework* in an ICEFR context.
- *Examples* provide specific illustrations to users on the application of each principle, based on situations drawn from practical experiences. Examples illustrate one or more points of focus of a particular principle. They are not designed to provide a comprehensive example of how the principle may be fully applied in practice.

Further, the *Compendium* illustrates how various characteristics of principles may be present and functioning[1] within a system of internal control relating to external financial reporting objectives.

Finally, the *Compendium* includes an index to all the examples, by topic, in Appendix A, organized by topics relating to the changes in business and operating environments noted in the Foreword to the *Framework*.

Limitations of Illustrations

The approaches and examples do not attempt to illustrate all aspects of the components and relevant principles necessary for effective internal control relating to external financial reporting objectives. Further, they are not sufficient to enable an organization to determine that each of the five components and relevant principles is present and functioning. Instead, the approaches and examples are intended to illustrate how principles may be present and functioning.

The approaches and examples are samples of activities for management to consider, rather than a complete or authoritative list. The components, principles, and definitions illustrated in the *Compendium* are consistent with those found in the *Framework*, and readers should refer to the *Framework* for a comprehensive discussion of how entities design, implement, and conduct a system of internal control, and for the requirements of effective internal control.

1 The *Framework* uses the terms "present and functioning" with respect to principles and components, and "selects, develops, and deploys" with respect to controls to effect principles.

Considerations for External Financial Reporting

This section considers some unique aspects of applying the *Framework* in the context of external financial reporting, especially the preparation of financial statements for external purposes.

Types of External Financial Reports

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

Financial Statements for External Purposes

Financial statements for external purposes are prepared in accordance with applicable accounting standards, rules, and regulations.[2] These financial statements may 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 or distributed through annual meetings, an entity's website, or other electronic media.

Another form of financial statements prepared for external purposes may be financial reports prepared in accordance with a special purpose framework, such as those established by taxing authorities or regulatory agencies, or those required through contracts and agreements. These financial reports are typically distributed to specified external users (e.g., reporting to a bank on financial covenants established in a loan agreement, reporting to a taxing authority in connection with filing tax returns, reporting on financial information to an energy regulatory commission).

Other External Financial Reporting

Other external financial reporting derived from an entity's financial and accounting books and records rather than from its financial statements for external purposes may include earnings releases, selected financial information posted to an entity's website, and selected amounts reported in regulatory filings. External financial reporting objectives relating to such other financial information may not be driven directly by regulators and standard setters, but typically stakeholders expect them to align with such standards and regulations.

2 Applicable accounting standards, rules, and regulations may include accounting principles generally accepted in the US (US GAAP), International Financial Reporting Standards (IFRS), Securities and Exchange Commission rules for disclosure, and others.

Objectives Established for External Financial Reporting

Regulators and accounting standard setters establish laws, rules, regulations and standards relating to the preparation of financial statements for external purposes. These form the basis upon which management specifies suitable objectives for the entity and its subunits. Regulators, standard-setting bodies, and other relevant third parties also establish criteria for defining the severity of, evaluating, and reporting internal control deficiencies. The *Framework* recognizes and accommodates their authority and responsibility as established through laws, rules, regulations, and standards.

In the case of an entity applying a law, rule, regulation, or standard, management should use only the relevant criteria contained in those documents when classifying the severity of internal control deficiencies, rather than the classifications set out in the *Framework*. The *Framework* recognizes that if a deficiency results in a system of internal control not being effective under such classification criteria then management cannot conclude that the entity has met the requirements for effective internal control as set forth in the *Framework*.

For example, a company that must comply with the classification criteria established by the United States Securities Exchange Commission (SEC) would use only the definitions and guidance set out for classifying internal control deficiencies as a material weakness, significant deficiency, or control deficiency.[3] If an internal control deficiency is determined to rise to the level of a material weakness, the organization would not be able to conclude that the entity's system of internal control over financial reporting has met the requirements for effective internal control as set out in the *Framework*. If an internal control deficiency does not rise to the level of material weakness the entity could achieve effective internal control over financial reporting.

Within the boundaries established by laws, rules, regulations, and standards, management exercises judgment to assess the severity of an internal control deficiency, or combination of deficiencies, in determining whether components are present, functioning, and operating together, and ultimately in concluding that the entity's system of internal control is effective.

Suitable Objectives of Financial Statements for External Purposes

Applicable Accounting Standards

In specifying the suitability of external reporting objectives relating to the preparation of financial statements for external purposes, management considers the accounting standards that apply to that entity and its subunits. Management then assesses and affirms the accounting principles that are appropriate in the circumstances. For example,

3 For the purposes of the *Compendium*, approaches and examples use the term "material weakness" as defined by the Securities Exchange Commission in the United States in the Securities Exchange Act of 1934 Rule 12b-2 [17 CFR 240.12b-2]. "Material weakness" means a deficiency, or a combination of deficiencies, in internal control over financial reporting such that there is a reasonable possibility that a material misstatement of the registrant's annual or interim financial statements will not be prevented or detected on a timely basis.

management may set an entity-level external financial reporting objective as follows: "Our company prepares reliable financial statements reflecting transactions and events in accordance with generally accepted accounting principles."[4]

Management specifies suitable sub-objectives for the entity's divisions, subsidiaries, operating units, and functions with sufficient clarity to support entity-level objectives. For example, a US company applies accounting principles generally accepted in the United States of America (US GAAP) to all subunits in preparing its consolidated financial statements; its subsidiaries also apply International Financial Reporting Standards (IFRS) to submit their subsidiary financial statements in various statutory filings in local jurisdictions.

Further, management assesses and affirms the suitability of the accounting principles to apply to transactions and events of the entity. For example, management specifies that FASB Accounting Standard Codification Topic 605 Revenue Recognition and SAB 101A Revenue Recognition in Financial Statements (US GAAP) or IAS 18 Revenue Recognition (IFRS) applies to all sales transactions as applicable to achieve the entity or subunits' respective external financial reporting objective.

In specifying and using applicable accounting principles, management exercises judgment, particularly relating to subjective measurements and complex transactions. For instance, management judgment is essential for making assumptions and using data in developing accounting estimates, in applying accounting principles to complex transactions and events, and in preparing reliable and transparent presentations and disclosures. In addition, management regularly updates the specified accounting principles for any changes in objectives established through law, rules, regulations and standards.

Considers Materiality

Financial statement materiality sets the threshold for determining whether a financial amount is relevant. Entities must consider suitable laws, rules, regulations, and standards promulgated by regulators and standard setters.[5]

Reflects Entity Activities

External financial reporting must reflect the entity's transactions and events. When preparing financial statements, management implicitly or explicitly considers suitable sub-objectives categorized into a set of assertions (e.g., existence and completeness of transactions) underlying the financial statements. Accounting standard setters may set forth these assertions as well as relevant qualitative characteristics for external financial reporting.

4 The United States Securities and Exchange Commission (SEC) "Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934" states that "Management is responsible for maintaining a system of internal control over financial reporting ('ICFR') that provides reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles."

5 For example, the SEC issued Topic 1M of the Staff Accounting Bulletins to provide guidance on assessing materiality and immaterial misstatements that are intentional. The International Accounting Standards Board provides a definition of materiality in paragraph QC11 of the "Conceptual framework for financial reporting 2010."

Management makes assertions regarding the recognition, measurement, presentation, and disclosure of accounts, transactions, and events included in the entity's financial statements. For example, one grouping of assertions[6] relating to financial statements is summarized as follows:

- *Existence or Occurrence*—Assets, liabilities, and ownership interests exist at a specific date, and recorded transactions represent events that actually occurred during a certain period.
- *Completeness*—All transactions and other events and circumstances that occurred during a specific period, and that should have been recognized in that period, have in fact been recorded.
- *Rights and Obligations*—Assets are the rights and liabilities are the obligations of the entity at a given date.
- *Valuation or Allocation*—Asset, liability, revenue, and expense components are recorded at appropriate amounts in conformity with relevant and appropriate accounting principles. Transactions are mathematically correct and appropriately summarized and recorded in the entity's books and records.
- *Presentation and Disclosure*—Items in the statements are properly described, sorted, and classified.

For example, management specifies sub-objectives for sales transactions that address relevant financial statement assertions such as:

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

Risks to Achieving Suitable Objectives

Risk of Material Omission or Misstatement

Management specifies suitable objectives and sub-objectives with sufficient clarity to be able to identify and analyze risks to the achievement of those objectives. Financial statements for external purposes are not considered reliable or fairly presented if material omissions or misstatements exist in one or more of the amounts or disclosures. In preparing financial statements, management should identify those risks that could, individually or in combination, result in a material omission within or misstatement of the financial statements.

6 These financial statement assertions are substantially consistent with those described in the standards of the American Institute of Certified Public Accountants, the Public Company Accounting Oversight Board, and the International Auditing and Assurance Standards Board.

Management's assessment of such risks involves a dynamic and iterative process. The initial assessment undertaken by management likely requires a comprehensive effort to identify and analyze the risk of not preventing or detecting, in a timely manner, a material omission within or misstatement of the entity's financial statements. The nature and frequency of performing ongoing and periodic risk assessments vary among entities, based on individual facts and circumstances.

Even though every entity requires a process to identify and assess the external and internal factors that contribute to the risk of achieving its objectives, specific changes and rates of changes in these factors (including those that could significantly impact internal control over external financial reporting) vary from entity to entity. For example, different entities and subunits may:

- Operate in many industries, markets, geographic territories
- Operate in multiple regulatory environments that promulgate different laws, rules, regulations, and standards
- Execute a multitude of contracts with customers, vendors, and others transacting business with the entity
- Acquire, divest, and restructure operations
- Deploy new and evolving technologies and information systems
- Experience turnover of management and other personnel involved in the system of internal control

Additionally, the size and complexity of the entity play a part in determining the nature and frequency of the risk assessment process. Large, complex organizations may require dedicated cross-functional and cross-territorial management and other personnel with necessary expertise to perform comprehensive risk assessments. Management of smaller entities may be able to perform its risk assessment through direct supervision and day-to-day involvement in operations.

Risk of Material Omission or Misstatement Due to Fraud

Fraudulent reporting can occur when an entity's reports are wilfully prepared with material omissions of misstatements. This may occur by the use of unauthorized receipts or expenditures, financial misconduct, or other disclosure irregularities. A system of internal control over external financial reporting is designed and implemented to prevent or detect, in a timely manner, any material omissions within or misstatements of the financial statements due to error or fraud.

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

- *Fraudulent External Financial Reporting*—An intentional act designed to deceive users of external financial reports and that results in a material omission within or misstatement of the external financial reports
- *Misappropriation of Assets*—Theft of the entity's assets where the effect may cause a material omission within and misstatement of the external financial reports

As part of the risk assessment process, the organization identifies the various ways that fraudulent financial reporting can occur, considering:

- Management bias in exercising judgment, for instance in selecting and using applicable accounting principles and developing significant estimates
- Degree of estimates and judgments underlying the accounting for and disclosure of transactions and events
- 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
- Attitudes and rationalizations by individuals engaging in or justifying inappropriate actions
- Nature of technology and management's ability to manipulate technology and information
- Unusual or complex transactions subject to significant management influence
- Vulnerability to management override and potential schemes to circumvent controls

Also, as part of the risk assessment process, the organization identifies risks pertaining to the completeness and accuracy of recording any material misappropriation of assets. Misstatements may arise from failing to record the material loss of assets or manipulating the financial statements to conceal such a loss.

Management Override

"Management override" refers to actions taken by management in an attempt to override the entity's controls for an illegitimate purpose such as personal gain or to enhance the presentation or disclosure of the entity's financial condition or results of operation. As part of its assessment of fraud risk, management considers the risk of management override of internal control. The board of directors or subset of the board (e.g., audit committee) oversees this assessment and challenges management when warranted. The entity's control environment can significantly influence the risk of management override. The risk of management override is especially relevant for smaller entities where senior management is typically selecting, developing, and deploying controls to effect principles.

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

Risk of Material Omission or Misstatement Due to Illegal Acts and Corruption

Illegal acts are violations of laws or governmental regulations that could have a material direct or indirect impact on the external financial report. Management considers various indicators to help identify risks relating to potential illegal acts, such as:

- Results of investigations by a governmental agency, an enforcement proceeding, or the payment of unusual fines or penalties
- Violations of laws or regulations cited in reports of examinations by regulatory agencies
- Large payments for unspecified services to consultants, affiliates, or employees
- Sales commissions or agents' fees that appear excessive in relation to those normally paid or the services actually received
- Unusually large payments in cash, purchases of bank cashiers' checks in large amounts payable to bearer, transfers to numbered bank accounts, or similar transactions
- Unexplained payments made to government officials, employees, or third parties
- Failure to file tax returns or pay government duties or similar fees
- Allegations by whistle-blowers or former employees

Management also considers possible corruption occurring within the entity. Corruption is generally relevant to the compliance category of objectives but could influence the control environment that affects achievement of the entity's external financial reporting objectives. This includes considering the incentives and pressures across the organization to achieve the entity's external financial reporting objectives while demonstrating adherence to the expected standards of conduct and the effect of the control environment, specifically actions linked to Principle 4 (Demonstrates Commitment to Competence) and Principle 5 (Enforces Accountability). Aspects of corruption typically relate to illegal acts that are considered in government statutes relevant to external financial reporting.

In assessing possible corruption, the entity is not expected to directly manage the actions of personnel within external parties, including those relating to outsourced service providers and other parties interacting with the entity. However, depending on the level of risk assessed, management may stipulate the expected level of performance and standards of conduct through contractual relations, and develop controls that maintain oversight of third-party actions. Where necessary, management responds to detected unusual actions of others.

Risk Response

When preparing financial statements for external purposes management exercises judgment in complying with external financial reporting requirements. Management considers how risks of material omission and misstatement should be managed across the entity. Management selects, develops, and deploys controls to effect principles within

each component to respond to assessed risks. Accordingly, management judgment is necessary in developing appropriate responses to risks of material omissions or misstatements, considering:

- Laws, rules, regulations, and standards that apply to the entity
- Nature of the entity's business and the markets in which it operates
- Scope and nature of the management operating model
- Competency of the personnel responsible for internal control over external financial reporting
- Use of and dependence on technology

Management's alternatives to respond to risks relating to external financial reporting objectives may be limited compared with some other categories of objectives. That is, management is less likely to accept a risk than to reduce the risk when considering the preparation of financial statements for external purposes. For instance, management may decide to outsource transaction processing to a third party that is better suited to perform the business process. However, management always retains responsibility for designing, implementing, and conducting its system of internal control even when outsourcing to a third party. For external financial reporting objectives, risk acceptance should occur only when identified risks could not, individually or in aggregate, exceed the risk threshold and result in a material omission or misstatement.

Management exercises judgment when selecting, developing, and deploying controls to mitigate risks. Accordingly, management's responses and actions depend on its assessed risks of material omission and misstatement, perceptions of benefits and costs of effective controls, and other facts and circumstances unique to the entity (e.g., management operating model, use of technology, competency of management and other personnel).

Further, management may enhance the efficiency in the design, implementation, and conduct of a system of internal control over external financial reporting by, for instance, acknowledging the following;

- Understanding the importance of specifying suitable objectives may focus management's attention on those risks and controls that are most important to achieving these objectives.
- Focusing on those areas of risk that exceed acceptance levels and need to be managed across the entity may reduce efforts spent mitigating risks in areas of lesser significance.
- Coordinating efforts for managing risks across multiple objectives may reduce the number of discrete, layered-on controls.
- Selecting, developing, and deploying controls to effect multiple principles may reduce the number of discrete, layered-on controls.
- Applying a common language—the *Framework*—encompassing operations, reporting, and compliance processes and controls may lessen the number of languages used to describe internal control across the entity.

Smaller Entities

The principles underlying the components of internal control apply to entities of all types and sizes. However, smaller entities may apply these principles using different approaches. For example, all public companies have boards of directors or other similar governing bodies with oversight responsibilities relating to the entity's external financial reporting. A smaller entity may have a less complex business model, organizational and legal structure, and operations, and more frequent communication with directors, enabling greater reliance on board oversight for achieving effective internal control.

The approaches contained within the *Compendium* are designed to be universal in nature and apply to any entity type or size. The examples, however, derived from actual situations, may include specific facts and circumstances that relate more to a larger entity. In most cases though, the examples translate well to applications for both smaller and larger entities.

Documentation

Two levels of documentation should be considered in relation to financial statements for external purposes:

- In cases where management asserts to regulators, shareholders, or other third parties on the design and operating effectiveness of its 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 present 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 and relevant principles are present and functioning and components are operating together is available and suitable to satisfy the entity's objectives.
- In cases where an external auditor attests to the effectiveness of the 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 control is effective, as defined in the *Framework* or as established by regulators, standard-setting bodies, or other third parties. 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, including the sufficiency of such documentation for those assertions. Management may also document significant judgments, how such decisions were considered, and the final decisions reached.

Structure of the *Compendium*

The *Compendium* illustrates through approaches and examples how the principles apply to external financial reporting objectives. Each chapter focuses on one of the five components of internal control and contains:

- A summary of the component that is consistent with the *Framework*
- A list of principles associated with that component
- A list of relevant approaches for applying principles in an external financial reporting context

Each principle is accompanied by a list of approaches. The approaches illustrate how organizations apply the principles in designing, implementing, or conducting certain aspects of internal control over external financial reporting. Approaches apply to any size or type of entity and illustrate important characteristics of each principle. The points of focus attached to each principle will assist users in understanding the linkages between the sample activities and these important characteristics of principles. Organizations will apply these approaches as appropriate depending on individual facts and circumstances, and application is likely to evolve as circumstances change over time. Note that the approaches included in the *Compendium* are not intended to be a comprehensive or authoritative list.

For each approach, one or more examples are provided to illustrate how an important aspect has been put in place by entities that prepare financial statements for external purposes. The examples are based on actual experiences of entities, although some details have been modified for the purposes of this publication (e.g., entity and personal names are fictional and should not be attributed to any specific entity). The examples are not intended to be construed as "best practices" or suggested solutions for users of the *Framework*. Further, the examples are not necessarily sufficient to demonstrate that a particular principle is present and functioning as defined in the *Framework*.

These approaches and examples are likely to be relevant to many types of entities (whether public, private, not-for-profit, or governmental) that aim to prepare financial statements for external purposes and other forms of external financial reporting. Where an example does not apply to all types of entities, this is noted. Finally, even though the approaches and examples primarily relate to preparing financial statements for external purposes, any entity seeking to design, implement, and conduct a system of internal control to achieve other external financial reporting objectives may find them beneficial.

2. Control Environment

Chapter Summary

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

Principles relating to the Control Environment component

1. The organization demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight 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 the objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Principles	Approaches
1. The organization demonstrates a commitment to integrity and ethical values.	• Establishing Standards of Conduct • Leading by Example on Matters of Integrity and Ethics • Evaluating Management and Other Personnel, Outsourced Service Providers, and Business Partners for Adherence to Standards of Conduct • Developing Processes to Report and Promptly Act on Deviations from Standards of Conduct
2. The board of directors demonstrates independence from management and exercises oversight for the development and performance of internal control.	• Establishing the Roles, Responsibilities, and Delegation of Authority of the Board of Directors • Establishing Policies and Practices for Meetings between the Board of Directors and Management • Identifying and Reviewing Board of Director Candidates • Reviewing Management's Assertions and Judgments • Obtaining an External View • Considering Whistle-Blower Information about Financial Statement Errors and Irregularities
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	• Defining Roles and Reporting Lines and Assessing Them for Relevance • Defining Authority at Different Levels of Management • Maintaining Job Descriptions and Service-Level Agreements • Defining the Role of Internal Auditors

Principles	Approaches
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with the objectives.	• Establishing Required Knowledge, Skills, and Expertise • Linking Competence Standards to Established Policies and Practices in Hiring, Training, and Retention Decisions • Identifying and Delivering on Financial Reporting–Related Training as Needed • Selecting Appropriate Outsourced Service Providers • Evaluating Competence and Behavior • Evaluating the Capacity of Finance Personnel • Developing Alternate Candidates for Key Financial Reporting Roles
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	• Defining and Confirming Responsibilities • Developing Balanced Performance Measures, Incentives, and Rewards • Evaluating Performance Measures for Intended Influence • Linking Compensation and Other Rewards to Performance

Demonstrates Commitment to Integrity and Ethical Values

Principle 1. The organization[7] demonstrates a commitment to integrity and ethical values.

Points of Focus

The following points of focus highlight important characteristics relating to this principle:

- Sets the Tone at the Top—The board of directors and management at all levels of the organization 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.

7 The term "organization" is used to collectively capture the board of directors, management, and other entity personnel as reflected in the definition of internal control.

Approaches and Examples for Applying the Principle

Approach: **Establishing Standards of Conduct**

Senior management, with guidance from the board of directors, defines and communicates expected standards of conduct for the organization, including any specific to those responsible for preparing external financial reporting. Such standards contain key provisions reflecting legal, ethical, and other expectations in the conduct of business and financial reporting, and articulate management's philosophy and guidance for avoiding moral hazards in the pursuit of objectives. They also leverage established professional codes of conduct, such as those associated with financial and managerial accounting, legal, information technology, or other professional organizations. To instill a common understanding of the company's standards, management develops various means for:

- Communicating and reinforcing the accountability for responsible conduct of all personnel
- Permeating standards of conduct throughout the organization, including guidelines for application to high-risk issues and geographies
- Setting the expectation that personnel raise issues or questions relating to the application of the defined standards
- Making explicit the consequences for deviations from standards of conduct at any level in the organization
- Ensuring that new and existing employees are trained on the entity's standards of conduct and continuing education, and providing appropriate briefings to third parties engaging in business with the company
- Developing performance evaluation processes and incentives (and service-level agreements as necessary) that promote the right behavior in pursuit of objectives
- Providing staff with ethics training opportunities to ensure that all employees have the knowledge to identify and deal with dilemmas

Sets the Tone at the Top
- Establishes Standards of Conduct
Evaluates Adherence to Standards of Conduct
Addresses Deviations in a Timely Manner

Example: **Defining, Communicating, and Regularly Updating the Code of Business Conduct and Ethical Standards**

The senior management of Zanzibar Co., a publicly traded company, has created, maintains, and distributes the company's code of business conduct and ethical standards to all employees and external parties acting on behalf of the company, and has posted it on the company website. The code of conduct is available in all relevant languages for ease of access and understanding by all within the global organization. The company requires all employees to complete periodic interactive web-based training sessions on various aspects of the code and ethical standards.

Furthermore, Zanzibar Co. provides a supplier code of conduct to its vendors as part of its service-level agreements, which provide a basis for evaluation alongside product/service delivery evaluation.

These documents emphasize that every individual is responsible for maintaining an ethical environment and reporting any ethical breaches. Service-level agreements and contracts with external parties include the relevant language to specify the company's expected standards of conduct and serve as a basis for evaluating adherence. The code also specifically sets out the expectation of reporting and resolving issues by providing clear information on how to ask a policy question or report a violation through an independent third party.

Senior management and the board of directors annually review and discuss any changes needed to the code or how it is administered, considering external and internal factors, including the coverage of the company's key risk areas, any known compliance issues, and results of monitoring activities. For instance, over time, Zanzibar Co. has added provisions to address new, applicable laws and has provided more guidance on what constitutes an appropriate gift or entertainment.

Approach: **Leading by Example on Matters of Integrity and Ethics**

- Sets the Tone at the Top
- Establishes Standards of Conduct

Evaluates Adherence to Standards of Conduct

Addresses Deviations in a Timely Manner

The CEO and key members of management at various levels in the organization articulate and demonstrate the importance of integrity and ethical values across the organization. The various forms and mechanisms used to do this may include:

- Communications from senior management that support the expected standards of conduct and that stay consistent as they permeate the organization
- Day-to-day actions and decision making at all levels of the organization that are consistent with the expected standards of conduct
- Interactions with suppliers, customers, and other external parties that reflect fair and honest dealings
- Performance appraisals and incentives that reinforce expected standards of behavior consistent with the entity's objectives at all levels of the organization
- Timely inquiries and investigations into any alleged conduct that is inconsistent with the entity's standards of conduct
- Corrective action when deviations from expected standards of conduct occur

While this approach can be synonymous with that of establishing standards of conduct when both operate effectively, history has shown instances where organizations define and communicate honorable standards of conduct, yet management does not internalize or exhibit these standards in its conduct, and therefore sets a different tone than what is expected.

Example: **Using a Company Newsletter to Reinforce Expectations of Integrity and Ethics**

Aerospacial S.A., a small supplier to the aerospace industry, uses its monthly newsletter to employees, outsourced service providers, business partners, and other external parties to emphasize the importance of exercising sound integrity and ethical values. Each edition of the newsletter contains a section related to ethical decision making and

consequences of violations of the code. The newsletter draws attention to the multitude of resources available to discuss and resolve ethical issues; it also reports what actions are taken by senior management when the code is violated at any level of the organization. The newsletter illustrates the open dialogue and resolution of issues that is actively promoted by senior management.

Examples of ethical dilemmas are provided, along with suggested resolutions. The newsletter points out that reports of violations originate from a variety of sources, including employees, managers, the company's anonymous hotline, and external parties. Responses range from no action (in cases where the violation is shown not to have occurred) to various levels of discipline, including dismissal.

Finally, the newsletter reminds all Aerospacial S.A. employees—from senior management to entry-level—that as part of their annual performance review they must certify that they have read the company's mission statement and code of conduct and that they comply with policies at all times.

Approach: **Evaluating Management and Other Personnel, Outsourced Service Providers, and Business Partners for Adherence to Standards of Conduct**

The board of directors and senior management evaluate adherence to the company's standards of conduct. This is accomplished in a variety of ways, which may include:

- Assessing results from training and ethics certification processes
- Considering anomalies in key performance indicators and internal analytical reviews of operational and financial information that could be a potential indicator of fraudulent financial reporting or other misconduct
- Considering the results from ongoing and separate evaluations of internal control, which include evaluations of internal control at outsourced service providers and business partners who provide information necessary to produce external financial reporting
- Analyzing issues and trends from hotlines and help lines made available within the organization that could indicate potential fraud occurrences and other ethical concerns
- Requesting feedback from meetings held with outsourced service providers and business partners when obtaining financial information or information that impacts the entity's internal control over external financial reporting

Sets the Tone at the Top
Establishes Standards of Conduct
• Evaluates Adherence to Standards of Conduct
Addresses Deviations in a Timely Manner

Example: **Conducting Ethics Audits**

The not-for-profit organization Partners for Development conducts scheduled audits to determine whether employees are receiving, understanding, and applying the board-approved standards of conduct. A completeness check is performed to verify that every employee has received and attested to these standards or otherwise provided a specific explanation that is then reviewed and addressed by senior management and the board. The audits also include non-employees and consultants from the organization's

IT service provider. The standards consist of three documents: the code of ethics and standards of personal conduct, the compliance policy statement, and the expected standards of conduct.

Partners for Development's purpose in conducting these audits is to determine if there are any shortcomings in understanding or instances of non-compliance and to use those findings to assess and correct any deficiencies in the organization's new-hire orientation, communications, training, and employee review processes. Upholding the organization's standards of conduct is intended to help safeguard against or escalate any instances of fraud, management override, or other illicit transactions and support complete, accurate, and reliable financial reporting to the organization's government sponsors.

Example: **Evaluating Misconduct Reported through an Anonymous Hotline**

All-World Food Distributors provides an anonymous hotline for employees to report potential fraud and other ethical concerns. The entity engages a third-party service provider to administer the hotline to provide the comfort of anonymity for its employees. This service immediately reports any potentially illegal acts or financial reporting improprieties directly to the company's legal department and audit committee. Issues and trends are analyzed and conclusions are reported to the audit committee of the board.

Approach: **Developing Processes to Report and Promptly Act on Deviations from Standards of Conduct**

Sets the Tone at the Top
Establishes Standards of Conduct
Evaluates Adherence to Standards of Conduct
• Addresses Deviations in a Timely Manner

Senior management develops and consistently follows a prescribed process and standard to promptly investigate, report, and take action to correct any violations to the standards of conduct occurring at any level of the organization, including outsourced service providers and business partners. The process may include:

- Having individuals who are independent of the alleged matter conduct the investigation (Note, however, where the deviation is deemed significant—due to the seriousness or pervasiveness of the allegation, degree of management involvement, regulatory interest, etc.—it may be necessary to have a board-led investigation, with a special committee that is independent of management.)
- Applying criteria to prioritize deviations (e.g., monetary value, patterns, trends, reputation impact)
- Investigating occurrences of possible violations to ensure a thorough understanding of issues and circumstances
- When applicable, assessing the financial statement impact and determining what internal controls over external financial reporting may have failed to detect the matter
- Developing appropriate support documentation and reporting
- Identifying and communicating with anyone under investigation (or after thorough investigation in instances of alleged fraud), and following up on any corrective

actions taken to remedy the matter in a consistent and timely basis and according to prescribed company guidelines

- Restricting access to sensitive information regarding the allegation to individuals authorized to handle the investigation
- Informing the board of deviations in the application of the standards and any waivers that may have been granted or that are being considered
- Determining how and when the violation will be communicated and if it will be made public
- Communicating to all company personnel that appropriate investigation and corrective actions have been taken
- Depending on the nature and pervasiveness of the deviation that has occurred, establishing remediation activities as needed to make retrospective corrections and forward-looking improvements

Remediation may address accounting corrections needed, process control enhancements, systems development or enhancements, accountability reinforcement, training, revisions to the standards of conduct, providing management, personnel or third parties with increased awareness of the importance of applying the standards, and other actions. The board reviews and approves the adequacy of remediation measures and progress reports.

Example: **Taking Action when Deviations Occur**

Best Fit Shoes has established policies and procedures to address serious improprieties or illegal acts by employees, such as theft or bribing a new supplier to secure a contract. The policy empowers the legal department to initiate the investigation together with the internal audit department or an external third party in order to understand, document, and report the facts of the alleged matter for evaluation and assessment.

Best Fit's policy clearly states that if such an illegal act or impropriety is confirmed, the company will terminate the employee, revoke all access privileges, and file formal charges with appropriate authorities. The policy also requires the human resources manager to document the situation and its resolution, analyze the root cause of the breach, and implement any additional remedial steps to avoid similar occurrences in the future. Progress reports are regularly provided to the audit committee.

During one instance, facilitation payments were made to obtain certain contracts, the policy was immediately applied, and an investigation was launched. The audit committee was notified and regularly presented with progress updates and the proposed corrective actions for approval.

Exercises Oversight Responsibility

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

Points of Focus

The following points of focus highlight important characteristics relating to this principle.

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

Approaches and Examples for Applying the Principle

Approach: **Establishing the Roles, Responsibilities, and Delegation of Authority of the Board of Directors**[8]

- Establishes Oversight Responsibility
- Applies Relevant Expertise
- Operates Independently
- Provides Oversight for the System of Internal Control

The roles, responsibilities, and powers of delegation of the board of directors are defined in its corporate bylaws and committee charters in accordance with applicable regulatory and listing requirements. For external financial reporting purposes, the board typically forms an audit committee whose responsibilities include overseeing:

- The effectiveness of internal control over external financial reporting, including the assessment of risks, significant deficiencies, and material weaknesses (if any)
- Management's assessment of any significant matters, considering the potential impact on financial reporting and need for corrective action
- The establishment of formal communication with management of the internal audit function to facilitate discussion of any sensitive issues
- The quality of financial reporting and disclosures
- The hiring of and payment to the external auditor

Audit committee members typically demonstrate independence of thought and substance by absence of any material financial or other personal ties to the company, which could impede their ability to provide unbiased guidance and oversight.

The responsibility of the board and audit committee is to oversee management's performance of internal control. The board must therefore retain objectivity in relation to management.

Example: **Reviewing and Documenting Key Activities of the Audit Committee**

Every year, the board of directors of Northern Power, a distributor of electricity, commissions an effectiveness evaluation of its audit committee. An independent consultant with expertise in governance reviews the means by which the audit committee fulfills its responsibilities, as set out in its charter. Specifically, it evaluates how the members of the audit committee:

- Oversee the quality and reliability of financial reporting and disclosures
- Understand the key risks facing the organization and the processes management uses to identify, assess, and manage risks, considering internal audit findings, litigation, compensation schemes, regulation, and compliance
- Evaluate organizational behavior, culture, and adherence to standards of conduct
- Challenge management and the external auditor in determining materiality for financial reporting purposes

8 In practice, many of the activities of the board of directors included here would be carried out by one of its committees, such as the audit committee.

- Assess reasonableness and appropriateness of critical accounting policies of the company
- Confirm or reject the basis for management estimates and proposed accounting policy changes before approving
- Evaluate, retain, or change external auditors
- Review audit plans
- Review management's assessment of internal control over external financial reporting

The results of the evaluation are used to determine whether the roles and responsibilities of the committee have been met and could result in committee member changes or impact remuneration. In addition to the annual review, every three years the company conducts a benchmark review against leading practices and refines its charter, as appropriate.

Example: **Reviewing Governmental Agency Financial Results and Underlying Internal Control**

Public Aid is a governmental agency that is subject to oversight by various bodies, representing knowledgeable and independent officials. In terms of its financial reporting, key roles include the following:

- The organization's deputy head is responsible for assuming overall stewardship for the integrity of the agency's financial management capabilities, and for signing off on all key external financial management representations and disclosures, including the Statement of Management Responsibility Including Internal Control over Financial Reporting.
- An audit committee, whose chairman is responsible for ensuring that the committee acts as an independent and objective advisor to the deputy head and provides guidance on the adequacy of the agency's system of internal control, financial reporting and disclosures.

The comptroller general is responsible for providing government-wide functional direction and assurance for financial management and stewardship over public resources, as assigned by the Treasury Board, in collaboration with other central agencies. He provides oversight of government-wide financial information systems and quarterly financial reporting. He monitors the qualifications and competence of the financial management community across government for all aspects of financial management and reports periodically to the Treasury Board on the state of financial management across government agencies.

Approach: **Establishing Policies and Practices for Meetings between the Board of Directors and Management**

- Establishes Oversight Responsibility
- Applies Relevant Expertise
- Operates Independently
- Provides Oversight for the System of Internal Control

The board of directors reviews and approves policies and practices that support the performance of internal control across the business in regular meetings between management and the board. The processes and structures particularly relevant to the audit committee of the board are those that provide:

- Appropriate forums to enable board members to ask probing questions of management
- A calendar that establishes the timing and frequency of meetings with management
- Expected practices to keep board members current on both emerging and adopted accounting standards and their impact on the entity's financial statements
- Procedures to review management's development and performance of internal control over external financial reporting
- Authority to engage experts as needed and oversight to ensure that management appropriately resolves matters raised by the board
- Criteria and procedures for calling special and/or urgent meetings as necessary
- Allocation of time in board meetings for discussions with external advisors, internal and external auditors, and legal counsel without management being present

The policies and practices are updated as needed to reflect changes in internal and external expectations, including rules and regulations.

Example: **Establishing an Audit Committee Meeting Calendar**

The audit committee of Outer Limits Innovations, an aerospace control systems supplier, uses its charter as guidance when setting its meeting dates and agendas. Fred Krahn, the chair of the committee, plans for at least one meeting during the year at which each responsibility set forth in the charter is discussed. This practice helps the audit committee to cover all relevant responsibilities and management to anticipate and plan for the committee's expectations. The meeting calendar, which is shown below, is periodically reassessed to adjust for emerging regulatory and technical matters that could affect the company or the industry.

	Frequency			Planned Meeting Quarter			
Audit Committee Issues	A	E	AN	1	2	3	4
Report of results of annual independent audit to the board	✓			✓			
Appointment of the external auditor	✓			✓			
Approval of external auditor fees for upcoming year	✓			✓			
Review of annual proxy statement audit committee report	✓			✓			
Assessment of the adequacy of audit committee charter	✓				✓		

	Frequency			Planned Meeting Quarter			
	A	E	AN	1	2	3	4
Approval of audit committee meeting plan for the upcoming year, confirm mutual expectations with management and the auditor	✓				✓		
Audit committee self-assessment	✓				✓		
Approval of guidelines for engagements of external auditors for other services (pre-approval policy)	✓			✓			
Approval of any non-audit services provided by outside auditors			✓				
Report of external auditor pre-approval status/limits		✓		✓	✓	✓	✓
Review of procedures for handling financial reporting errors or irregularities	✓				✓		
Oversee fraud risk assessment process	✓			✓			
Review the charter of the internal audit function	✓			✓			
Review the internal audit plan	✓			✓			
Approval of minutes of previous meeting		✓		✓	✓	✓	✓
Report quarterly matters to the board (chair)		✓		✓	✓	✓	✓
Schedule executive session of committee members			✓				
Schedule executive sessions with the chief audit executive	✓		✓	✓			
Other matters			✓				
Financial Management							
Annual report, 10-K, and proxy statement matters	✓			✓			
Quarterly report earnings review with management and external auditor, pre-approval of external auditor professional activities		✓		✓	✓	✓	✓
Assessment of system of internal control	✓			✓			
Status of significant accounting estimates, judgments and special issues (e.g., major transactions, accounting changes, SEC issues)			✓				
Other matters (adequacy of staffing, succession planning, etc.)			✓				

A = Annually E = Each Meeting or Conference Call AN = As Necessary

Example: Preparing Effectively for Meetings

The audit committee of Millennium Lighting, a manufacturer of lighting and ventilation equipment, is chaired by Janis White, a CPA with financial reporting expertise and previous public accounting experience. Ms. White regularly distributes to the committee members any updates from management on technical matters, such as new accounting standards or developments affecting the company and related financial statement implications.

Before each committee meeting, she circulates the draft agenda both to the committee members and the external auditors to solicit their input on any additional technical accounting agenda items they would like to discuss. Ms. White is committed to keeping open channels of communication with the external audit engagement partner and the

company's chief audit executive to ensure she receives timely updates on any discussions occurring with management as technical matters emerge. Internal audit, litigation, and corporate social responsibility are a few of the areas that are regularly solicited for input by the board or audit committee.

Approach: **Identifying and Reviewing Board of Director Candidates**

The board of directors periodically assesses and confirms its collective ability to provide effective oversight. Through independent review and self-assessment it determines the adequacy of its composition, whether it has sufficient independent members, and the appropriate expertise.

To meet the entity's external financial reporting objectives, the board of directors identifies certain board candidates who are independent of both management and the entity and who have requisite financial reporting and other relevant expertise. These members are typically assigned to the audit committee.[9] Such expertise may be established through professional networks and organizations and by educational institutions whose missions are aligned to the advancement of the financial reporting profession.

The board reviews the results of due diligence performed on potential board candidates and confirms their competence and ability to remain unbiased. The procedures to ensure that potential board members meet the defined criteria may include:

- Evaluating the key risks facing the organization and accordingly defining board member profile requirements
- Performing background checks and obtaining independent references
- Reviewing current affiliations and directorships to ensure independence relative to management and the entity
- Considering skills and expertise, ranging from financial to regulatory and various technical knowledge needed to understand the issues that could affect the company's external financial reporting
- Validating that any credentials and certifications held demonstrate an achieved competence level
- Reviewing information about financial and other relationships with the company, its external auditors, or management
- Using an independent nominating committee or search firm to oversee due diligence procedures
- Evaluating periodically the due diligence procedures used for identifying potential directors, including checking that an individual director's certifications are complete, up-to-date, and comply with the entity's ethics guidelines and independence rules

Establishes Oversight Responsibility

- Applies Relevant Expertise
- Operates Independently

Provides Oversight for the System of Internal Control

9 Standard setters, regulators, or listing agencies may have specific requirements for director independence, qualifications, and the makeup of the audit committee, which will vary by jurisdiction/country.

Example: **Changing the Board Composition of a Closely Held Company**

Giante Ore is a mining exploration company whose shares are traded on an "over-the-counter" bulletin board. Giante Ore has long maintained a board of directors that includes three of the CEO's family members and three outside, but not independent, directors: the company's outside legal counsel, a venture capitalist, and a personal friend of the CEO.

Giante Ore recognized that it needed to strengthen its control environment and board effectiveness. To that end, it revisited its board structure. The three relatives and one personal friend of the CEO left the board and have been replaced by four independent directors, all of whom are financially literate. One of the four has specific financial expertise. These directors have now been appointed to a newly formed audit committee with its responsibilities set forth in a charter.

Example: **Assessing and Disclosing Director Qualifications**

When Greene Inc. needs to identify new members for its board, it follows a detailed procedure to ensure the best possible candidates are chosen. The nominating committee works with the human resources department, the legal department, and an independent executive search firm to identify candidates and conduct due diligence in support of the interest of the company in its short- and longer-term objectives. The key skills it has identified are financial literacy, liquidity risk management expertise, business continuity planning, and corporate social responsibility reporting experience that reflects the business performance expectations of the company's stakeholders.

The same team conducts an annual review to ensure that board members continue to have the requisite competence and independence given the entity's stakeholder needs. The senior management of Greene Inc. provides the results of the review in its public filings.

Approach: **Reviewing Management's Assertions and Judgments**

Establishes Oversight Responsibility

- Applies Relevant Expertise

Operates Independently

- Provides Oversight for the System of Internal Control

The board demonstrates an appropriate level of skepticism of management's assertions and judgments that affect financial reporting by asking probing questions. In particular, the audit committee of the board seeks clarification and justification of the company's process for:

- Selecting and implementing accounting policies
- Determining critical accounting estimates
- Making key assumptions used in the application of technical accounting and reporting matters
- Evaluating other risks facing the organization, with the potential impact on financial reporting

Example: **Reviewing Financial Statement Estimates**

Custom Engineering manufactures specialty polymer products. The audit committee meets regularly with management to review the reasonableness of management's assumptions and judgment used to develop significant estimates. The committee then meets privately with the external auditor to discuss its assessment of management's estimates and the related impact on financial reporting.

This practice is carried out for all assumptions related to key financial statement accounts, disclosures, and relevant assertions most subject to management judgment and bias. For example, for Custom Engineering's annual goodwill evaluation, management provides relevant information on any specialists engaged to assist the company, key judgments and assumptions included in the company's discounted cash flow model, plausible sensitivity scenarios that were considered, and confirmation of the appropriate technical accounting standard applied.

Approach: **Obtaining an External View**

The audit committee of the board meets regularly with internal and external auditors as well as independent reviewers, in private when necessary, to review and discuss such topics as:

- Key risks facing the organization
- Audit scope and testing plans
- Basis for definition of materiality threshold
- Changes in accounting policies
- Assumptions in models and calculations
- Resources and staffing
- Organization and culture
- Management's assessment of internal control over financial reporting
- Significant audit findings
- Quality and reliability of financial reporting and disclosures

Establishes Oversight Responsibility
Applies Relevant Expertise
Operates Independently
• Provides Oversight for the System of Internal Control

Example: **Interacting with Auditors**

Sara Greenburg is the chair of the audit committee of Seaworthy Solutions, a marine construction services provider. In accordance with the audit committee charter, she arranges for the committee to meet quarterly with the external auditor to discuss a wide range of issues such as audit scope, testing plans, internal control over external financial reporting, quality of financial reporting, and audit findings and recommendations. She is responsible for coordinating the audit committee's evaluation of the external auditor. She bases her evaluation on a number of considerations, including the firm's reputation, the qualifications of the audit partner and team, knowledge and experience in the company's industry, and the firm's quality control procedures. Ms. Greenburg believes that these interactions, supplemented as needed with interim conversations,

effectively positions her to monitor the external auditor's performance and make an informed judgment on any need to modify or terminate the relationship.

The audit committee also regularly meets with Seaworthy's chief audit executive to ensure that the same oversight objectives of the internal audit function are attained. The chief audit executive reports directly to the audit committee to enable an objective mindset within the internal audit organization and to facilitate the escalation of issues independent of management, if so required.

Approach: **Considering Whistle-Blower Information about Financial Statement Errors and Irregularities**

Establishes Oversight Responsibility
Applies Relevant Expertise
Operates Independently
• Provides Oversight for the System of Internal Control

The audit committee considers information obtained from the company's whistle-blower and anti-fraud programs (or similar processes) to monitor the risks in misstatements in financial reporting. These may include risks of inappropriate acts by staff and management override of controls. The audit committee reviews any whistle-blower allegations and evaluates management's analysis of significant matters, potential impact on financial reporting, and corrective actions being taken.

Example: **Assessing the Potential of Management Override**

Start-up Inc. is a privately held company that has grown rapidly and now faces heightened competition and declining margins. The owners have become increasingly concerned about the potential for fraud and management override to make quarterly results look more favorable and meet performance targets. In response, Human Resources has made a help line available to management and staff, and an external service provider now provides a hotline for anonymously reporting breaches of ethics and integrity that could impact external financial reporting. The owners review all allegations received, assign the cases for investigation, and review the findings to understand the motivations, opportunities, and rationalizations for management override and how those activities might be concealed, and to ensure prompt corrective action is taken.

Example: **Investigating and Reporting Whistle-Blower Allegations**

Generation Now is an electricity transmission and distribution company that periodically receives calls on its whistle-blower hotline. The business ethics committee chaired by the general counsel reviews the logs of all calls and determines the appropriate course for follow-up action. Matters are opened and assigned to internal audit for investigation and proposed resolution by senior management and the board, as appropriate. Investigations are carried out by internal auditors or others who are independent of the issue. Every quarter, internal audit, working in conjunction with the general counsel, provides a status report of progress and proposed resolutions relating to each call. The board and management determine the final resolution and oversee any follow-up actions.[10]

10 This example is continued in Chapter 6, Monitoring Activities, to illustrate how monitoring activities may assess whether controls to effect principles in the control environment are deployed as intended (see page 147).

Establishes Structure, Authority, and Responsibility

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

Points of Focus

The following points of focus highlight important characteristics relating to this principle:

- Considers All Structures of the Entity—Management and the board of directors consider the multiple structures used (including operating units, legal entities, geographic distribution, and outsourced service providers) to support the achievement of objectives.
- Establishes Reporting Lines—Management designs and evaluates lines of reporting for each entity structure to enable execution of authorities and responsibilities and flow of information to manage the activities of the entity.
- Defines, Assigns, and Limits Authorities and Responsibilities—Management and the board of directors delegate authority, define responsibilities, use appropriate processes and technology to assign responsibilities, and segregate duties as necessary at the various levels of the organization:
  - *Board of Directors*—Retains authority over significant decisions and reviews management's assignments and limitations of authorities and responsibilities
  - *Senior Management*—Establishes directives, guidance, and control to enable management and personnel to understand and carry out their internal control responsibilities
  - *Management*—Guides and facilitates the execution of senior management directives within the 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

Approaches and Examples for Applying the Principle

Approach: **Defining Roles and Reporting Lines and Assessing Them for Relevance**

- Considers All Structures of the Entity
- Establishes Reporting Lines
- Defines, Assigns, and Limits Authorities and Responsibilities

Senior management prepares organizational charts to document, communicate, and enforce accountability for the achievement of the entity's financial reporting objectives. The organizational charts can be used to:

- Set forth assignments of authority and responsibility
- Ensure duties are appropriately segregated
- Establish reporting lines and communication channels
- Define the various reporting dimensions relevant to the organization
- Identify dependencies for roles and responsibilities involved in financial reporting as well as those accountable for external parties

Each unit or department within the entity that is relevant to external financial reporting aligns its roles and responsibilities to processes supporting the financial reporting objectives. Senior management and the board of directors verify that accountability and information flow within each of the various organizational structures (by business segment, geographical location, legal entity, or other) continually support the achievement of the entity's existing financial reporting objectives. Existing structures are periodically assessed for relevance considering changes in the entity or the environment in which it operates to ensure such alignment.

Example: **Reorganizing to Support Control Structure**

Before Harmony Homes Real Estate became a public company, a wide range of the employees reported to the owner and CEO, Milton Chang, and the business structures in the US and in Asia were loosely connected. During the plans to go public, Mr. Chang, with the board's guidance, took steps to strengthen the organizational structure to better support both operations and financial reporting objectives. Management created three departments to oversee its core business activities: sales and customer service, purchasing/inventory, and production. Geographic governance structures were also established to oversee operations by jurisdiction and facilitate reporting to local regulators and other stakeholders. The managers charged with leading each of these departments and territories, as well as the managers of key staff functions, documented each person's responsibility in the processes. Job descriptions, including internal control responsibilities, were developed to support full understanding of each person's role.

The clear statement of roles helps to ensure responsibilities are carried out in support of the organization's objectives. It also provides the basis for risk assessment, control activities, information and communication, and monitoring activities along different dimensions simultaneously.

Example: **Redefining Roles with CEO and Board Input**

Due to significant changes within the company and the industry, Pieter Jenssen, CEO of transportation services provider General Trucking, recognized the need to redefine the role of each position within the company's mid- to high-level management team, especially within the finance and accounting function. His initiative was launched at an off-site meeting where the goals and objectives of the business were reviewed and realigned with managers' specific roles and responsibilities, including those related to the financial reporting process. Two board members attended the meeting to serve as a sounding board, and all participants reached a shared understanding on how they will function and interact with one another in the future. The results of the meeting were communicated to other managers throughout the organization. The communication included a description of organizational lines by product line, geography, and management structure. It also included associated roles, responsibilities, and communication procedures, incorporated into policies that were made readily accessible on the company's intranet.

Approach: **Defining Authority at Different Levels of Management**

The board of directors outlines its oversight authority for financial reporting over senior management through its charter. When assigning authorities and responsibilities, management considers the impact on the control environment and the importance of effectively segregating duties. Policy documents define cascading levels of authority, checks, and balances for authorizing transactions, and accounting and reporting of financial results. Such authority and responsibility is deliberately limited in order to balance the need for the efficient achievement of objectives against the risks that could result from unmonitored inappropriate conduct. Management empowers employees to correct problems or implement improvements in their assigned business process as necessary.

- Considers All Structures of the Entity
- Establishes Reporting Lines
- **Defines, Assigns, and Limits Authorities and Responsibilities**

Example: **Maintaining an Authority and Approval Matrix**

Muell AG, a waste management company maintains policies that detail the monetary commitment and transaction approval authorities of its managers on a per occurrence basis. Managers who exceed their individual transactions authority must obtain approval from the appropriate higher-level management, which in some cases includes the board of directors. These authority and responsibility policies exist for a broad range of the company's business functions, including mergers and acquisitions, sales and marketing, purchasing, risk management, labor, capital expenditures (including landfills), IT expenditures, and leases. The policies are updated when necessary to reflect changes in the business, and any revisions require the approval of the chief accounting officer.

Considers All Structures of the Entity

Establishes Reporting Lines

- Defines, Assigns, and Limits Authorities and Responsibilities

Approach: **Maintaining Job Descriptions and Service-Level Agreements**

Based on the delegated authority levels, management maintains job descriptions to outline financial reporting responsibilities, and updates them when needed. In addition, management provides sufficient direction to ensure that employees recognize their responsibility for internal control and the importance of applying appropriate diligence and business judgment when they carry out their assigned job responsibilities.

For key financial reporting positions, the board of directors reviews management's descriptions of the related authorities and responsibilities and considers how those positions affect the strength of internal control over external financial reporting.

When applicable, the responsibilities of externally sourced support personnel are outlined through service-level agreements, specifically targeting timeliness and the quality of financial reports generated.

Example: **Aligning Roles and Responsibilities with Objectives**

The senior management at MNO Games, a games software developer, has recognized that the company's recent significant growth is causing many of the roles and responsibilities of its management executives to be no longer relevant. Responsibilities of the controller and CFO overlap, systems for product being sold through new channels are not adequately reviewed, and the CEO is not effectively communicating initiatives and agreements across the senior management team.

In response, the senior managers have initiated a project to realign responsibilities among its leadership team. The goals are to adequately support financial reporting objectives, with clear lines of reporting supported by new written job descriptions. The project has already resulted in a new company policy for MNO Games that requires each business unit manager to maintain the updated job descriptions and organizational charts depicting positions and lines of reporting within the unit.

Example: **Maintaining Control while Engaging Outside Service Providers**

SureSafe provides identify-theft protection and credit management services to credit card companies and has decided to outsource its payroll and 401(k) plan administration to capitalize on cost savings, ease access to relevant specialists for technical and administrative questions, and improve segregation of duties between its key payments and collections processes.

SureSafe identified a small reputable company, J.K. Green and Associates, as one that would meet its processing, reporting, and internal control needs. The service-level agreement signed by both parties specifies each party's expectations and responsibilities for the services provided and internal control over the outsourced business processes.

Approach: **Defining the Role of Internal Auditors**

In companies with formal internal audit functions (which can vary from an individual assigned with internal audit responsibilities to a formal department), the board of directors empowers the internal audit function to carry out its purpose, authority, and responsibilities with direct access to the audit committee and/or the board of directors. The board or audit committee is actively involved in reviewing the company's risk assessment, ensuring that the internal audit plan provides adequate assurance on the adequacy of coverage of key risk areas, and overseeing internal audit compensation to ensure it is structured in a manner that supports the need for objectivity.

Example: **Reviewing and Approving the Internal Audit Plan**

Sam Murphy, the chief audit executive officer of Pine Tree Real Estate, annually presents an internal audit plan to the CEO and audit committee for review and approval. The audit plan includes the scope, work plan, staffing, and budget for the coming year, as well as any modifications needed in the charter to define roles and responsibilities.

The audit committee reviews and approves the plan, recognizing that it may need to be revisited periodically to respond to significant changes in the company, such as new product lines, acquisitions, unexpected regulatory issues, etc. The audit committee regularly assesses the independence of the chief audit executive and evaluates the activities of the internal audit function.

Demonstrates Commitment to Competence

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

Points of Focus

The following points of focus highlight important characteristics relating to this principle:

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

Approaches and Examples for Applying the Principle

Approach: **Establishing Required Knowledge, Skills, and Expertise**

- Establishes Policies and Practices
- Evaluates Competence and Addresses Shortcomings
- Attracts, Develops, and Retains Individuals
- Plans and Prepares for Succession

The audit committee of the board reviews and approves the competency requirements of all individuals serving in key financial reporting and internal audit roles and for all members of the audit committee. These are based on applicable laws and regulations, and on the expertise needed for applying the entity's existing policies and practices related to external financial reporting.

Management develops and maintains policies and practices that reflect the organization's values and objectives. For instance, job descriptions capture the expectations in terms of the knowledge, skills, expertise, and credentials needed to effectively carry out responsibilities for each financial reporting position.

The finance department regularly reviews the entity's accounting and reporting policies and practices, and updates these as necessary to keep pace with internal expectations and external factors, including changes in technical standards and regulatory requirements.

The human resources department periodically updates materials outlining the company's policies and procedures on attracting, training, coaching, evaluating, and retaining personnel.

Example: **Periodically Reviewing Policies**

Asha Sandhu leads the human resources department of NetTech Industries, a provider of networking technology platforms. She works with the business unit and functional leaders to define the roles and responsibilities of personnel and related job descriptions that are aligned to the company's objectives. For instance, she helps the chief financial officer establish the job descriptions of financial reporting personnel, tying back to the performance of accounting, reporting, and internal control policies and procedures. She also brings together the respective owners of policies and procedures to review the continued relevance and adequacy of content, considering relevant factors such as organizational changes, new accounting standards, or revised disclosure requirements. She ultimately facilitates the update process, communications, and training, as necessary.

Approach: **Linking Competence Standards to Established Policies and Practices in Hiring, Training, and Retention Decisions**

- Establishes Policies and Practices
- Evaluates Competence and Addresses Shortcomings
- Attracts, Develops, and Retains Individuals
- Plans and Prepares for Succession

Policies and practices that represent the entity's competence standards for financial reporting positions are used as a basis for human resource and employee compliance activities, which may include:

- Selecting and interviewing candidates
- Performing background/reference checks
- Making hiring, retention, promotion, and termination decisions

- Developing training curricula
- Setting certification expectations
- Conducting exit interviews to uncover any concerns related to the entity's internal control over external financial reporting

Example: **Recruiting and Retaining Key Financial Reporting Positions**

The CFO of La Porte, a garage door manufacturer, is looking to fill the position of controller for its affiliate in France. The job requires someone with in-depth experience in local public filing reporting compliance requirements, a high level of integrity, and sound ethical values.

La Porte has screened candidates through interviews by a cross-section of leaders of key departments, the human resources department running background checks, and the CFO interviewing the candidates' references. The assessment criteria included the extent of each candidates' technical accounting knowledge, the complexity of issues they had dealt with in their career to date, their willingness to learn and take on new challenges, and the ability to make ethical business decisions.

When hired, the successful candidate will be expected to participate in several relevant conferences throughout the year to maintain a current level of knowledge of industry and financial reporting matters and recognize that he or she is valued as an important asset to the company.

Example: **Defining Performance Expectations**

A leading provider of consumer credit, Credit Safe, believes in establishing and reinforcing a culture in which its employees are aware of performance expectations and requirements. To that end, annual performance objectives are established and documented for each employee. For example, employees working in finance and internal audit roles are expected to either work toward obtaining a certification or attend a requisite amount of continuing education training to maintain existing certifications.

Credit Safe periodically evaluates every employee's performance and tracks it against established objectives. Management provides feedback and guidance to help employees achieve the objectives. At the end of each year, an employee's performance is rated as one of several categories: superior, exceeds expectations, meets expectations, needs improvement, or unsatisfactory.

Approach: **Identifying and Delivering Financial Reporting–Related Training as Needed**

Establishes Policies and Practices

- Evaluates Competence and Addresses Shortcomings
- Attracts, Develops, and Retains Individuals

Plans and Prepares for Succession

Training needs are identified and delivered to targeted personnel. These address regulatory expectations, emerging accounting and reporting standards, and in-house input on areas that require improvement. Training needs are reprioritized as necessary in response to how often applicable changes occur, both within and outside the organization.

Example: **Implementing Complex Accounting Standards**

Orex, a mining exploration company that makes extensive use of stock options in compensating its senior employees, has been subject to a pronouncement on accounting for stock compensation. Max Tellemann, the chief financial officer, and Arlene Shreve, the company controller, attended an external training session on the pronouncement, which included working through examples of how the standard would be applied in various cases. Mr. Tellemann and Ms. Shreve assessed the suitability of their company's practices by performing an impact analysis based on expert opinions and trade publications that discuss expected impacts and pitfalls. They then revised existing policies and procedures and provided communications and training to affected personnel.

This intensive training has provided senior management of Orex with the confidence that their CFO and controller now have sufficient knowledge to make informed decisions on the proper application of the standard. Documentation of the training attended has been tracked and included in Ms. Shreve's and Mr. Tellemann's employee files.

Approach: **Selecting Appropriate Outsourced Service Providers**

Management identifies the required skills and experience necessary to support the entity's external financial reporting objectives. It then decides whether to internally retain people with the skills and experience or to outsource to a third party. The suitability of a third party is determined not only by assessing skills and experience, but also by considering the entity's policies on using vendors and on ethical standards. The contractual arrangement with the outsourced service provider captures these competence requirements and provides the basis for the entity to periodically assess the outsourced service provider's continued commitment to competence.

Establishes Policies and Practices

- Evaluates Competence and Addresses Shortcomings
- Attracts, Develops, and Retains Individuals

Plans and Prepares for Succession

Example: **Retaining External Tax Assistance**

Compu Services, a developer of analytical software products, currently has limited tax accounting expertise among its staff. The finance director therefore sought to contract with a third-party accounting firm, SMR Ledger, LLP, to review its tax provisions. SMR Ledger is a different accounting firm from the Compu Services auditor.

For successful selection and use of the vendor's services, management was careful to verify that the vendor met the suitability standards set forth in Compu Services' policies. Being directly affected by the quality of the control procedures carried out by the vendor, the CFO spends time with the vendor to understand any assumptions used in models or calculations, particularly as they may impact financial reporting. Indeed, while Compu Services' management chooses to outsource certain tax activities, it remains responsible for the effectiveness of relevant controls regardless of where they are operated. The company therefore requests annual independent certifications of the vendor's internal control effectiveness.

Establishes Policies and Practices
• Evaluates Competence and Addresses Shortcomings
Attracts, Develops, and Retains Individuals
Plans and Prepares for Succession

Approach: **Evaluating Competence and Behavior**

To instill a common understanding and application of expected competence and behavioral standards, management consistently communicates expectations through policies and conducts practices and evaluates employee adherence by:

- Developing incentives and rewards that consider the multiple dimensions of conduct and performance
- Reinforcing expectations of continued demonstration and strengthening of expected levels of competence
- Ensuring individual and team goals in support of the achievement of the entity's objectives are defined, use observable metrics, and are communicated to each employee
- Developing a performance appraisal process that confirms employee knowledge of both their progress against their goals and their status within the organization
- Conducting periodic performance reviews and evaluating employees relative to their assigned roles to confirm that the employees' skills are appropriate for their current job responsibilities
- Making appropriate advancement or termination decisions based on performance reviews
- Changing the performance appraisal process as needed based on lessons learned or changes in strategy and operating objectives
- Continually endorsing behavior that is consistent with competence standards, and discouraging inconsistent behavior

Using the same criteria, the board of directors evaluates the competencies of individuals serving in key financial reporting roles, such as the chief executive officer, chief financial officer, and chief audit executive.

Example: **Periodically Assessing Performance**

City Government periodically reviews the performance of its employees who are responsible for owning, executing, or testing financial reporting controls. Performance is evaluated against expectations that are established at the beginning of each year. The progress achieved on needed improvements is reviewed with employees at the end of each quarter, and a more formal annual review process occurs following the year-end reporting cycle. An employee's career advancement is based on the overall performance rating. Management identifies specific areas for improvement and professional growth, which employees can address with training and development steps, as jointly agreed with the respective manager in the context of City Government's finance function and overall performance objectives.

Example: **Audit Committee Review of Managers' Roles**

The bylaws of Lead Products Co. specify the responsibility of the audit committee of the board for reviewing the principal roles and responsibilities of key financial reporting senior management. To this end, the chair of the audit committee meets annually

with the company's human resources director, chief audit executive, and legal counsel to review the roles, responsibilities, and performance of the various company managers. The review focuses on aligning respective managerial responsibilities with Lead Products' organization chart, and the managers' expertise and experience in carrying out the responsibilities. The audit committee also evaluates the independence of the relationship between management and the chief audit executive, considering input from the chief financial officer and other primary customers of internal audit services.

Approach: **Evaluating the Capacity of Finance Personnel**

Senior management evaluates the capacity of personnel who are involved in recording and reporting financial information, and in designing and developing financial reporting systems including underlying IT systems. Senior management assesses the department's ability to identify issues, articulate positions supported by the relevant literature, and stay abreast of technical financial reporting developments. Considerations when assessing the adequacy of staffing levels and competence of financial reporting personnel include the extent of technical skills, nature and frequency of their training, workload, and the number of personnel dedicated to financial reporting.

Establishes Policies and Practices

- Evaluates Competence and Addresses Shortcomings

Attracts, Develops, and Retains Individuals

Plans and Prepares for Succession

Example: **Assessing the Adequacy of Staffing Levels for Financial Reporting**

The senior management of Tall Tree Finance, an investment bank and institutional securities company, annually assesses the adequacy of staffing levels of its key financial reporting function to understand and manage effectively the company's current business activities, related accounting questions, and IT implementation challenges. The audit committee oversees this assessment.

In particular, the assessment considers how adequately personnel respond to emerging accounting, reporting, and internal control issues. Senior management uses the results of this assessment to make decisions on staff training, reassignments, or other organizational changes.

Example: **Aligning Competencies with Key Financial Reporting Positions**

The start-up company of Wireless Data Communications has seen its revenue double over the last several years, and business transactions and processing have become significantly more complex. Because of these evolving corporate needs due to the rapid growth, it is essential for employee competencies in key financial reporting positions to be aligned with increased levels of complexity.

Consequently, the CEO, CFO, and vice-president of human resources together annually review employee job descriptions, workload, and performance assessments. During a recent review, they determined that the company's controller, hired initially to perform basic accounting and bookkeeping functions, no longer had the expertise needed for the associated financial reporting responsibilities. The company has now assigned the controller to a position better suited to his skills, and hired an individual with the requisite competencies as controller.

Establishes Policies and Practices
Evaluates Competence and Addresses Shortcomings
Attracts, Develops, and Retains Individuals
• Plans and Prepares for Succession

Approach: **Developing Alternate Candidates for Key Financial Reporting Roles**

The board of directors identifies the essential roles for the functioning of the business, including the CEO and the CFO, deemed most important to the achievement of the entity's financial reporting objectives. For each of those roles, management defines succession plans to ease any future transition and to mitigate the risk of not meeting financial reporting objectives. The board of directors oversees this process to ensure that management has properly assessed and managed the risks associated with succession planning.

Example: **Addressing Succession Planning**

North-to-South Healthcare has an aging workforce and realizes it needs a succession plan. Over the past year it developed a "talent management strategy," which formalizes a succession planning framework and a process and leadership development program. The succession plan identifies those positions and external parties that are critical to the organization.

North-to-South has assessed current personnel to determine potential candidates for those critical positions in the future. The company has developed customized competency models for each of the critical positions and assessed the competencies of current staff as possible future candidates. For each of the identified candidates, an individual development plan and a leadership program have been established. These include experiential learning programs and executive mentoring programs.

For outsourced service providers or business partners critical to the performance of external financial reporting (such as information technology, payroll, accounts payable processing), North-to-South has defined contingency plans to allow for alternative arrangements in the event that such external parties become unavailable. The management member responsible for the relationship is also responsible for maintaining and executing the contingency plan, as necessary.

The talent management strategy has allowed North-to-South to confidently plan for the future.

Enforces Accountability

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

Points of Focus

The following points of focus highlight important characteristics relating to this principle:

- 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.

Approaches and Examples for Applying the Principle

Approaches: **Defining and Confirming Responsibilities**

- Enforces Accountability, through Structures, Authorities, and Responsibilities
- Establishes Performance Measures, Incentives, and Rewards
- Evaluates Performance Measures, Incentives, and Rewards for Ongoing Relevance
- Considers Excessive Pressures
- Evaluates Performance and Rewards or Disciplines Individuals

Management develops descriptions of various roles to reinforce its responsibility for effective internal control over external financial reporting. In pursuit of the entity's objectives, the board of directors and senior management maintain a philosophy and operating style that demonstrate a strong commitment to ethics, integrity, and competence.

Periodically, the CEO and CFO, as the parties ultimately responsible for internal control, request individuals within the entity to confirm accountability and represent that they have fulfilled their internal control responsibilities during any given period of time, highlighting any exceptions.

Example: **Cascading Responsibilities throughout the Organization and Certifying Results**

Auto Services is a publicly traded multinational automotive manufacturing, leasing, and sales organization that administers an annual goal-setting and performance evaluation process to help its employees be aware of the risks inherent in their day-to-day business decisions.

Representing its products adequately to its customers, saying no to bribes and other illicit practices, and delivering timely products or services in accordance with quality standards are the explicit expectations of the company and of each one of its representatives. Management communicates and reinforces these messages continually and holds its people accountable to these measures in their day-to-day decisions and overall risk and performance results, which it tracks proactively through client satisfaction dashboard reports and reactively through incident reporting. The company requires its employees to sign off on the goals mutually agreed to with management at the beginning of the year, recognizing that these may be revisited during the year as necessary to respond to changes in the business, and on their achieved performance at year-end.

Goals are defined, performance is evaluated, and employees are held accountable within the local organizational structure and within their functional reporting structure.

The chief financial officer further requires each of his finance managers to certify to him the absence of any instances of fraud, the effectiveness of the internal control over external financial reporting, and the reliability of the financial results produced.

Approach: **Developing Balanced Performance Measures, Incentives, and Rewards**

- Enforces Accountability, through Structures, Authorities, and Responsibilities
- Establishes Performance Measures, Incentives, and Rewards
- Evaluates Performance Measures, Incentives, and Rewards for Ongoing Relevance
- Considers Excessive Pressures
- Evaluates Performance and Rewards or Disciplines Individuals

Senior management defines performance measures, incentives, and rewards that are:

- Aligned with the entity's ethical values
- Developed at all levels of the entity that management deems necessary to support and ensure accountability toward meeting both the entity's short-term and longer-term objectives

- Balanced to include both financial and non-financial measures
- Incorporated into the entity's hiring, evaluation, and promotion structures

Senior management subsequently reports to the board what factors were considered in developing the performance measures, incentives, and rewards and how they are expected to drive the desired behavior.

Example: **Defining and Communicating the Basis for Reward**

Modern Financial Services has implemented a rewards system that requires the achievement of defined performance measures and encourages departments to monitor the effectiveness of their internal control systems and to self-report possible control deficiencies or opportunities for enhancement. This encouragement comes in the form of a policy that gives departments credit in the internal audit grading system for self-reported deficiencies. Any deficiencies that are identified through internal audit procedures, rather than through a department's monitoring efforts, are counted against the score.

The credit does not preclude the internal audit department from reporting specific deficiencies to management or the board when warranted, but it does positively affect the grading system, which can affect departmental compensation and benefits. The result is that Modern Financial Services is more likely to identify control deficiencies before they can become material to the organization.

Approach: **Evaluating Performance Measures for Intended Influence**

The board of directors and management periodically evaluate the appropriateness of performance measures used to determine whether they have the intended influence on how people respond to pressures, incentives, and rewards. This evaluation may include:

- Reassessing the relevance of performance measures considering industry trends, regulatory changes, or changes in the entity's objectives
- Considering past financial errors, ethical violations, and instances of non-compliance and whether the established measures could have caused excessive pressures to override controls
- Engaging external parties to conduct benchmarking and to interview employees
- Monitoring the changing sources of threats that cause pressure to bypass established controls or take shortcuts
- Considering whether the selection of accounting policies has been unduly influenced by the established performance measures
- Using the assessment to make changes in performance measures and associated hiring, evaluation, and promotion structures

The board of director's oversees the periodic assessment to ensure it has been completed, and may subsequently approve compensation plans. The board also provides oversight to ensure that the performance measures and compensation plans

Enforces Accountability, through Structures, Authorities, and Responsibilities
Establishes Performance Measures, Incentives, and Rewards
- Evaluates Performance Measures, Incentives, and Rewards for Ongoing Relevance
- Considers Excessive Pressures
Evaluates Performance and Rewards or Disciplines Individuals

established for senior management are appropriately aligned with the entity's strategic objectives and balanced to promote the desired accountability without causing excessive pressure that could lead to fraudulent financial reporting.

Example: **Establishing and Overseeing Performance Measures, Incentives, and Rewards**

The board of directors of A-Z Corp. has established a human resources compensation committee, which meets to establish compensation for the executive officers. It has been granted substantial discretion to determine all other bonuses under approved incentive plans.

The compensation committee routinely reviews the performance goals and awards for ongoing relevance and to determine whether they create unnecessary pressures or unintended consequences. It continually focuses on identifying those short-term sales objectives that may cause management to take undue risk, cut corners, or commit fraud that could harm the company's sustainable growth objectives.

Based on these reviews, goals and awards are modified as necessary, and changes are approved by the board of directors annually. The performance goals and awards consist of the following and are subject to audit:

- Earnings per share
- Audit scores
- Customer care
- Efficiency ratio
- Stock price (peer group comparison)

In addition, individual employee performance goals are determined annually in discussion between the employee and the manager. They are then submitted to the human resources department for review, and to the compensation committee for approval.

Any incentive compensation that is approved and ratified by the board is distributed to individuals annually.

Approach: **Linking Compensation and Other Rewards to Performance**

Management designs objective employee evaluation and compensation systems that periodically provide individual rewards, or disciplinary actions, as necessary. Decisions about both rewards and disciplinary actions are based on established objectives, including the individual's adherence to the standards of conduct and performance toward the entity objectives regarding internal control over external financial reporting.

Enforces Accountability, through Structures, Authorities, and Responsibilities

Establishes Performance Measures, Incentives, and Rewards

Evaluates Performance Measures, Incentives, and Rewards for Ongoing Relevance

Considers Excessive Pressures

- Evaluates Performance and Rewards or Disciplines Individuals

Example: **Aligning Incentives with Ethics and Values**

Timber Co., a forest products company, structures its bonus plan to have 30% of the potential incentive award directly related to the demonstration of the company's core

values. Information items that Timber Co. values are specific comments on how management does or does not reflect values are captured through employee feedback.

During the employee performance review and appraisal process, management provides feedback about the extent to which each employee has performed in accordance with the company's core values of sound integrity and ethics.

Example: **Providing Recognition for Suggestions Made to Enhance Internal Control**

Medic Quest, a private company that researches, develops, produces, and markets medical scanning equipment, encourages its employees to identify and submit suggestions for improving internal control, including internal control over financial reporting. Employees are rewarded in the form of company awards and/or cash bonuses for ideas that are used.

3. Risk Assessment

Chapter Summary

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

Principles relating to the Risk Assessment component

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

Principles	Approaches
6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	• Identifying Financial Statement Accounts, Disclosures, and Assertions • Specifying Financial Reporting Objectives • Assessing Materiality • Reviewing and Updating Understanding of Applicable Standards • Considering the Range of Entity Activities
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.	• Applying a Risk Identification Process • Assessing Risks to Significant Financial Statement Accounts • Meeting with Entity Personnel • Assessing the Likelihood and Significance of Identified Risks • Considering Internal and External Factors • Evaluating Risk Responses
8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.	• Conducting Fraud Risk Assessments • Considering Approaches to Circumvent or Override Controls • Considering Fraud Risk in the Internal Audit Plan • Reviewing Incentives and Pressures Related to Compensation Programs
9. The organization identifies and assesses changes that could significantly impact the system of internal control.	• Assessing Change in the External Environment • Conducting Risk Assessments Relating to Significant Change • Considering Change through Succession • Considering CEO and Senior Executive Changes

Specifies Relevant Objectives

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

Points of Focus

The following points of focus highlight important characteristics relating to this principle:

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

Approaches and Examples for Applying the Principle

Approach: **Identifying Financial Statement Accounts, Disclosures, and Assertions**

- Complies with Applicable Accounting Standards
- Considers Materiality
- Reflects Entity Activities

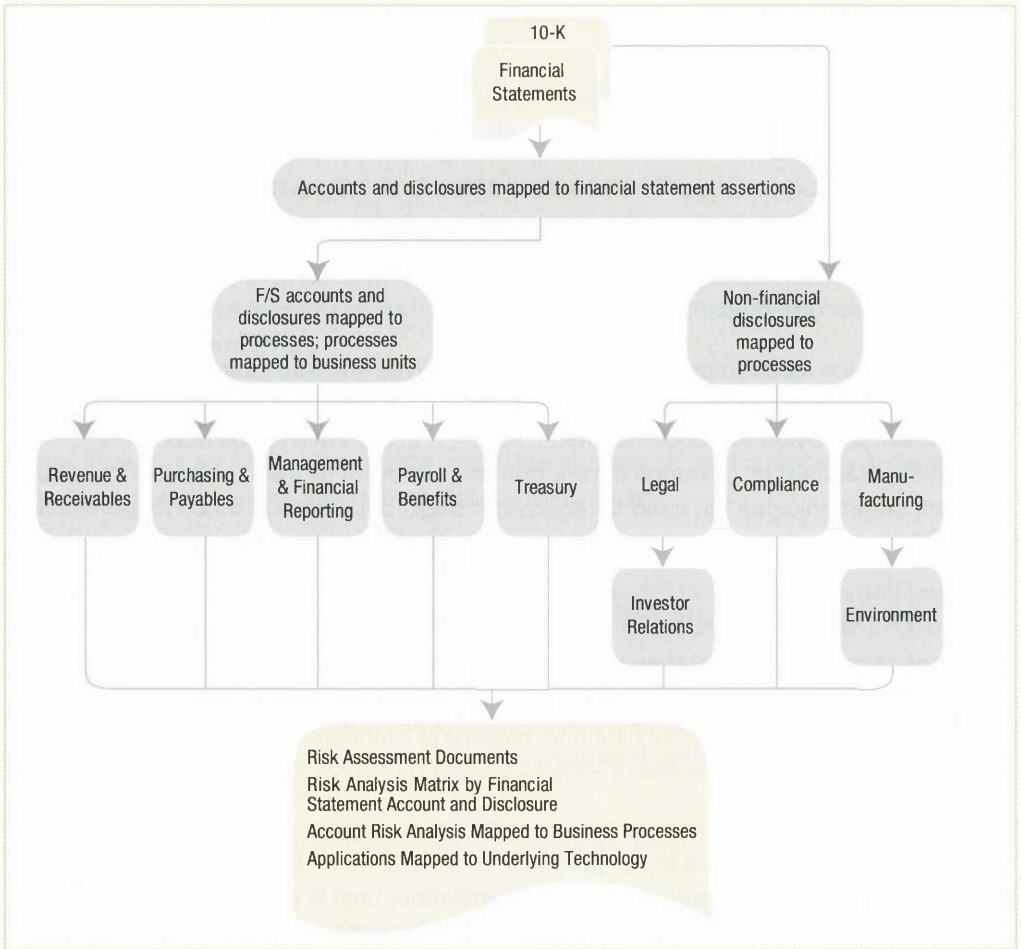
Management specifies objectives relating to the preparation of financial statements, including disclosures, and identifies significant financial statement accounts based on the risk of material omission and misstatement (which includes consideration of materiality). Management identifes for each account and disclosure relevant assertions, underlying transactions and events, and processes supporting these financial statement accounts. The entity uses financial statement assertions relevant to its financial statement accounts and disclosures.

Example: **Linking Accounts, Assertions, and Risks**

As part of its risk assessment, the management of A-Middle Equipment, a 900-person manufacturer of heavy-duty transmission equipment, uses the following financial reporting assertions:

- Existence
- Completeness
- Rights and obligations
- Valuation or allocation
- Presentation and disclosure

A-Middle's management considers the level of materiality when reviewing the company's activities and interim reports and determining whether all significant risks and accounts have been captured. This information is used as a guideline in focusing on detailed risks within each financial statement line item and disclosure. Further, management also considers non-financial disclosures reported in the company's 10-K. This approach is illustrated on the following page.



Approach: **Specifying Financial Reporting Objectives**

Management specifies a high-level financial reporting objective that forms the basis for all other sub-objectives. In specifying objectives, management has documented objectives that are specific, measurable, attainable, relevant, and time-bound (SMART). Management, as part of internal control, assesses whether the objectives are consistent with accounting principles that are relevant for that entity and appropriate in the circumstances.

- Complies with Applicable Accounting Standards
- Considers Materiality
- Reflects Entity Activities

Example: **Specifying Objectives**

Management and the board of directors of H_2O To Go, a bottled water company, set as the entity's broad external financial reporting objective to prepare reliable financial statements in accordance with US Generally Accepted Accounting Principles (GAAP). Management subsequently specified the suitable financial reporting objectives and sub-objectives for all significant accounts and activities of H_2O To Go's worldwide business, including sales, purchasing, and treasury. These objectives and sub-objectives include accounting policies, financial statement assertions, and qualitative characteristics

relating to its accounts and activities. For instance, management has specified objectives relating to:

- Sales existence and completeness financial statement assertions for all sales transactions recorded during the period[11]
- Purchasing completeness and accuracy of financial statement assertions for all purchasing transactions recorded during the period
- Treasury valuation and allocation financial statement assertions for all investments held and recorded as of period end

Annually, finance management reviews these objectives and sub-objectives for ongoing relevance and suitability with respect to the company's accounts and activities. Where changes are expected to occur—for instance, the adoption of a newly published accounting standard or guidance or new commercial event or trend—appropriate management communicates the need to reconsider these objectives to those responsible for the objective-setting process.

Example: **Assessing the Suitability of Specified Objectives**

The management of Valley Services, a supplier of high-end home theatre systems, set as the entity's broad financial reporting objective to prepare reliable financial statements in accordance with International Financial Reporting Standards (IFRS). This objective was cascaded into various areas of Valley Services business, including sales.

Within the sales process, management accepts deposits from one frequent customer, Hall Electronics, which relate to the purchase of several home theater systems. Valley Services sets aside the theater systems in its inventory until Hall Electonics requests delivery, usually within thirty days. Valley Service must either refund to Hall Electonics the cash or provide a relacement home theater system if a system is damaged or lost prior to delivery.

Management had previously established a policy where revenue was recognized upon payment for goods, regardless of whether the goods were delivered. In assessing the suitability of the objectives specified for financial reporting, the controller, Alex Robertson, determined that this policy may not be in accordance with IFRS. Consequently, he requested senior management to review this policy in conjunction with the objective-setting process. In addition, he advised the internal audit group, which then monitored the resolution of this matter.

Approach: **Assessing Materiality**

Complies with Applicable Accounting Standards
- Considers Materiality

Reflects Entity Activities

Management assesses materiality of significant accounts, considering both quantitative and qualitative factors. In conducting this assessment, management may consider factors such as:

- Who uses the financial statements (i.e., creditors, stockholders, suppliers, employees, customers, regulators)

11 For purposes of this example, not all relevant financial statement assertions have been included.

- Size of financial statement elements (i.e., current assets, current liabilities, total assets, total revenues, net income) and financial statement measures (i.e., financial position, financial performance, and cash flows)
- Uniqueness of the transaction(s)
- Difficulty in valuing the balance or specific transactions
- Trends (i.e., earnings, revenues, cash flows)

Example: **Assessing Materiality for a Private Company Financial Statement**

The management of Bottomer Holdings, a private owner and renter of residential apartments, recently installed coin-operated laundry facilities in several of its buildings. A contractor installed and maintains the machines and will be paid a monthly amount plus a percentage of revenue earned through laundry services.

Looking at this new source of potential revenue relative to the income statement, Bottomer Holdings considered the effect on its total revenues and net income and has now concluded that the laundry revenue is expected to generate $150,000 to $200,000 of revenue per year.

Management has considered the overall materiality of this account using the quantitative measure of $500,000. Management also considered other qualitative factors and determined that this new source of income would:

- Not change a loss into income—the company has been profitable over the past five years.
- Not impact compliance with loan covenants and other contractual agreements—none of the mortgages on the buildings would require changes in loan repayment rates based on higher income levels.
- Not impact management's compensation, including on-site property management staff—the additional income would have an insignificant impact on the management bonus plan.

Based on the assessment, management has concluded that the new source of income is not material to the overall financial statement presentation. Accordingly, in specifying its external reporting objectives, management has incorporated this new source of revenue into its overall revenue objectives as determined by Generally Accepted Accounting Principles but has not set out new, unique objectives for laundry-related revenue.

Approach: **Reviewing and Updating Understanding of Applicable Standards**

Management reviews publications from professional bodies for updates in accounting pronouncements relevant to the business. Periodically, management presents to the audit committee an analysis of changes released or emerging issues that may significantly impact financial reporting and notes any significant differences from accounting

- Complies with Applicable Accounting Standards

Considers Materiality

Reflects Entity Activities

policies of similar entities. For entities that have multiple reporting obligations, such as statutory reporting in international locations, management assesses the requirements relative to the respective divisions or operating units.

Example: **Reviewing Financial Accounting Policies**

Celia Mendez is the controller of a $100 million biotechnology company. She reviews its accounting principles by considering:

- Policies selected that are acceptable according to the applicable standards (US GAAP)
- Situations where multiple acceptable alternatives are available and the rationale for selecting one policy over another
- Differences in its accounting policies from those of its peers

Management discusses significant accounting policies with the audit committee on an annual basis.

Example: **Reviewing and Updating Understanding of Applicable Standards**

The management of Middle Ocean Inc., an $800 million industrial products company, regularly reviews the publications from professional bodies for updates in accounting pronouncements relevant to its business. The controller, Sandy Wong, and the CFO, Fred Jazbowski, also subscribe to and review periodic email updates on standards that may be of interest. Each quarter Ms. Wong presents to the company's audit and disclosure committees, which consist of key management members, her analysis of any changes that will immediately impact financial reporting, and any emerging issues that may impact financial reporting in the future. As part of her standard procedures and before any change is implemented, Ms. Wong also communicates to these two committees what impact any updated or new standard will have on the company's financial statements, systems, and processes.

Example: **Reviewing and Updating Statutory Reporting Requirements**

Fred DeQuincy is the local controller of an international subsidiary of a multi-billion-dollar consumer products company. In his annual reviews of the accounting principles used for statutory reporting, Mr. DeQuincy considers the following:

- Consistency with the company's consolidated accounting standards
- Required differences as a result of the adherence to different standards
- Where differences are required, the alternatives that are available and the rationale for selecting one policy over another
- Where differences are required, identifying the policies selected by other companies within an identified peer group

Once he has completed his review, Mr. DeQuincy communicates the differences and the rationale for selection to the corporate controller.

Approach: **Considering the Range of Entity Activities**

Management, with the oversight of the audit committee, considers the range of the entity's activities to assess whether all material activities are appropriately captured in the financial statements. Management considers whether the presentation and disclosure of the financial statements enable the intended users to understand these material transactions and events.

Complies with Applicable Accounting Standards

Considers Materiality

- Reflects Entity Activities

Example: **Considering the Range of Assessment Activities**

Build Free Co. produces large-building products. The management of Build Free reviews its financial statements on a quarterly basis. The purpose is twofold:

- To ensure all significant activities are included
- To analyze its various business units for new and discontinued product developments and changes in the company's markets, ensuring that they are conveyed appropriately in the financial statements

In addition, the audit committee discusses with management how any significant activities that it is aware of will be included in the financial statements.

Identifies and Analyzes Risks

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

Points of Focus

The following points of focus highlight important characteristics relating to this principle:

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

Approaches and Examples for Applying the Principle

Approach: **Applying a Risk Identification Process**

Management includes a risk identification process that identifies risks of material omission and misstatement and the likelihood of occurrence of the risks to relevant financial statement assertions for each significant account and disclosure. In preparing this analysis, management considers the business processes and business units supporting financial statement accounts and disclosures. The process of identifying the supporting business units includes discussions with each business unit or process leader. It also includes identifying the information technology systems that support those business processes that are relevant to the external financial reporting objectives.

- Includes Entity, Division, Operating Unit, and Functional Levels
- Analyzes Internal and External Factors
- Involves Appropriate Levels of Management
- Estimates Significance of Risks Identified
- Determines How to Respond to Risks

Example: **Analyzing Risk across Functions**

Lionel Tetrault is the CFO of Shark Tank Co., a firearms manufacturer. He convenes a working session of the department heads of marketing, production, information technology, human resources, and administration to perform a risk analysis by functional department. Risks are rated from 1 (least risk) to 5 (most risk) based on potential impact on financial reporting and likelihood of occurrence. After the discussion sessions, the participants document the results in a table that outlines each specific risk together with the rating and factors contributing to the rating.

For example, the risk of material omission and misstatement due to revenue recognition was rated as 4 (medium-high). Contributing to this assessment was consideration of the likelihood and impact of the organization failing to:

- Transfer ownership on specific sales in accordance with revenue recognition accounting standards for goods sold on consignment
- Account for complex sales promotions and discounts completely and accurately
- Update IT systems to account for complex revenue transactions that could lead to inappropriate recognition of revenue

Approach: **Assessing Risks to Significant Financial Statement Accounts**

Management identifies risks to the achievement of financial reporting objectives by considering risk factors related to each significant financial statement account and the associated financial statement assertions. The process of identifying and analyzing risk considers both quantitative and qualitative factors, including the following:

- *Impact on Financial Statement Accounts*—The potential impact on financial reporting objectives is measured quantitatively. Each account is assessed in relation to its respective category, such as total assets or revenues. Management also qualitatively assesses the potential for certain accounts to be understated. Considering the quantitative and qualitative characteristics, management categorizes accounts as high, medium, and low, based on their impact on the financial statements. Where risks vary by sub-account, management considers risk at that level.

Includes Entity, Division, Operating Unit, and Functional Levels

- Analyzes Internal and External Factors

Involves Appropriate Levels of Management

- Estimates Significance of Risks Identified

Determines How to Respond to Risks

- *Account Characteristics*—Management considers internal factors such as volume of transactions through an account, judgment required, and complexity of accounting principles. Management also considers external factors such as economic, competitive, and industry conditions; the regulatory and political environment; any new regulations affecting the account; and changes in technology, supply sources, customer demands, or creditor requirements.
- *Business Process Characteristics*—Management identifies business processes that generate transactions in each of the financial statement accounts, considering factors such as complexity of the process, centralization versus decentralization, IT systems supporting the process, changes made or new processes added, and interaction with external parties such as vendors, creditors, shareholders, or customers.
- *Fraud Risk*—For susceptible accounts, management assesses the risk of misstatements due to fraud.[12]
- *Entity-Wide Factors*—Management considers internal entity-wide factors such as the nature of the company's activities, employees' access to assets, number and quality of personnel and levels of training provided, changes in information systems, and organizational changes (e.g., changes in senior personnel or responsibilities). These factors are considered in relation to their effect on account characteristics, business process characteristics, and fraud risk.

Example: **Assessing Risks to Significant Financial Statement Accounts**

The management of Bachmann Tools, a hand tool importer, manufacturer, and distributor, identifies risks to the achievement of financial reporting objectives by considering risk factors related to each significant financial statement account and disclosure item. The criteria used for assessing risk are similar to those shown above in Approach: Assessing Risks to Significant Financial Statement Accounts. Management also links each account balance to financial statement assertions.

The resulting risk assessment is illustrated below. (Note: Additional detail underlying the risk assessment would typically be present supporting this analysis. For purposes of this example the summary of the assessment is provided.)

12 As noted in Principle 8, identifying and analyzing fraud risks are integral parts of the risk assessment process.

Risk Identification and Analysis by Account and Disclosure

Financial Statement Account/ Disclosure	As % of Total	Impact on F/S[13]	Account Characteristics	Business Process Characteristics	Fraud Risk	Entity-wide Factors	Overall Rating	Relevant Assertions[14]				
								E	C	V/A	R&O	P&D
BALANCE SHEET												
ASSETS												
Cash & Cash Equivalents	6%	M	H	M	H	M	H	✓	✓	✓	✓	✓
Accounts Receivable	30%	H	H	H	H	L	H	✓	✓	✓	✓	✓
Prepaid Expenses	4%	L	M	L	L	L	L	✓	✓	✓	✓	✓
Inventory	35%	H	M	M	M	L	M	✓	✓	✓	✓	✓
Property & Equipment	15%	H	L	L	L	L	L	✓	✓	✓	✓	✓
Intangible Assets	10%	H	M	M	M	M	M	✓	✓	✓	✓	✓
Total Assets	**100%**											

13 Note: Each heading used in this table is explained above in Approach: Assessing Risks to Significant Financial Statement Accounts.

14 Existence, Completeness, Valuation or Allocation, Rights and Obligations, and Presentation and Disclosure

Financial Statement Account/ Disclosure	As % of Total	Impact on F/S	Account Characteristics	Business Process Characteristics	Fraud Risk	Entity-wide Factors	Overall Rating	Relevant Assertions				
								E	C	V/A	R&O	P&D
LIABILITIES												
Accounts Payable	25%	H	H	L	M	L	M	✓	✓	✓	✓	✓
Accrued Expenses	15%	H	M	M	H	L	H	✓	✓	✓	✓	✓
Warranty	15%	H	M	M	M	L	M	✓	✓	✓	✓	✓
Long-Term Debt	10%	H	L	L	L	L	M	✓	✓	✓	✓	✓
Total Liabilities	**65%**											
SHAREHOLDERS' EQUITY												
Common Stock	5%	M	M	M	L	L	L	✓	✓	✓	✓	✓
Retained Earnings	30%	H	L	L	L	L	M	✓	✓	✓	✓	✓
Total Liabilities and Equity	**100%**											

Financial Statement Account/ Disclosure	As % of Total	Impact on F/S	Account Characteristics	Business Process Characteristics	Fraud Risk	Entity-wide Factors	Overall Rating	Significant Assertions				
								E	C	V/A	R&O	P&D
INCOME STATEMENT												
REVENUES												
Product Sales	85%	H	H	H	H	M	H	✓	✓			✓
Repair Services	15%	H	H	M	M	M	H	✓	✓			✓
Total Revenue	**100%**											
Cost of Goods	40%	H	H	H	H	M	H	✓	✓			✓
OPERATING EXPENSES												
Compensation & Related Benefits	28%	H	H	H	M	L	M	✓	✓			✓
Marketing & Selling Expenses	7%	M	M	L	L	L	M	✓	✓			✓
G&A Expense	3%	L	M	L	L	L	L	✓	✓			✓
Depreciation & Amortization	2%	L	M	M	L	L	L		✓			
Total Operating Expenses	**40%**											
OTHER EXPENSES												

Financial Statement Account/ Disclosure	As % of Total	Impact on F/S	Account Charac-teristics	Business Process Charac-teristics	Fraud Risk	Entity-wide Factors	Overall Rating	Significant Assertions				
								E	C	V/A	R&O	P&D
Interest Income/ (Expense)	5%	L	L	M	L	L	M	✓	✓			✓
Income Taxes Expense	5%	L	M	H	M	L	H	✓	✓			✓
Net income	**10%**											
Total, as percent of Revenue	**100%**											

Example: **Using Risk Ratings**

The management of Sure Health Care has developed a rating system to show general measures and trends of relevant risks. It now uses the ratings to determine which processes require more in-depth attention. The relevance of the financial reporting assertions for the related accounts is also considered. Management reviews the identified risks and provides a rating based on the inherent and residual risks to the entity; it updates these ratings periodically.

The information technology managers of Sure Health Care meet with finance personnel every month to discuss process, changes, and projects in each functional area relating to financial reporting. The meetings are used to update team members and discuss issues or changes to the processes. Additionally, management meets with outside legal counsel every quarter to discuss the effects of any external regulatory changes that may impact financial reporting.

The ratings are as follows:

- *High*—Critical processes that require in-depth documentation, including a matrix to describe identified risks and controls that mitigate these risks. Process maps and narratives are also developed to describe the flow of transactions and to identify control points. Controls are identified as preventive or detective, and manual or computer-based. Policies and procedures that guide employees in applying control activities are identified.
- *Medium*—Processes for which management prepares process documentation that includes a matrix to describe identified risks and controls that mitigate the risks. Process maps and narratives are developed where applicable at a high level. Policies and procedures are identified and documented, but in less formal, summary form.
- *Low*—Processes that require minimal process documentation, which identify policies and procedures and applicable controls.

Approach: **Meeting with Entity Personnel**

Key finance personnel meet regularly with:

- Executive management to identify initiatives, commitments, and activities affecting risks to financial reporting
- Information technology personnel to monitor changes in information technology that may affect risks related to financial reporting
- Human resources staff to identify and assess how changes in personnel and movement in positions may affect competencies needed for internal control over external financial reporting
- Legal counsel to stay abreast of legal and regulatory changes
- Other members of the entity as areas of focus are identified by executive management

- Includes Entity, Division, Operating Unit, and Functional Levels

  Analyzes Internal and External Factors
- Involves Appropriate Levels of Management

  Estimates Significance of Risks Identified

  Determines How to Respond to Risks

Example: **Analyzing Risk for Information Technology**

McFayden Inc. is a spirits distillation and distribution company with a dedicated information technology department. Risk assessment is driven by the number and complexity of applications that support the financial reporting process. This approach helps the company establish which information systems management relies on for financial reporting. Prior to implementing new systems, and whenever significant changes to existing systems are planned, McFayden Inc. takes the following steps:

- IT personnel meet with the business process owners to consider IT process–related risks. At these meetings, IT personnel learn how application data is used in the financial reporting process, identify risks of inaccurate or incomplete processing, and consider existing general computer controls in determining whether computer application controls or related user controls need to be enhanced.
- Relevant IT staff, along with business process owners, map the related applications to the operating systems, databases, and supporting IT processes, and consider inherent risks and what improvements are needed.
- IT personnel with relevant experience review opportunities to automate manual controls to improve efficiency.
- IT discusses activities with finance personnel.

Approach: **Assessing the Likelihood and Significance of Identified Risks**

Includes Entity, Division, Operating Unit, and Functional Levels

Analyzes Internal and External Factors

Involves Appropriate Levels of Management

- Estimates Significance of Risks Identified
- Determines How to Respond to Risks

Management analyzes the significance of identified risks based on the likelihood of the risk occurring and the inherent risk of a material omission and misstatement to the entity's external financial reporting objectives. Based on the outcomes of the analysis, management determines how to manage the risks to a tolerable level.

Example: **Identifying and Responding to Risk**

A social service organization with significant amounts of federal funding and operations in several foreign countries prepares an annual risk assessment of its financial reporting processes in each country. Risk factors considered include the following:

- Size of program and growth/downsizing
- Nature of funding in the country and types of program (federal or local)
- Nature of transactions
- Quality and timeliness of reporting (program and accounting)
- Quality of management and turnover (finance and program)
- Results of prior year's internal, external, and statutory audits
- Perception of country's political, social, and economic environment
- Oversight provided by funding sources in the countries

The risk assessment is prepared by the CFO, Gerald Timewell, and the COO, Inga Karran, with input from many others within the organization. The resulting assessment, for financial reporting purposes, considers the above risk factors in determining the significance of risks of material omission and misstatement related to the financial reporting assertions. For instance, management increased the assessed risk relating to existence of federal funding revenue from moderate to high after considering that there is:

- Uncertainty over the ongoing viability of funding programs in some foreign countries
- Irregular timing of funding payments in some foreign countries
- Weaknesses noted in a recent internal audit review

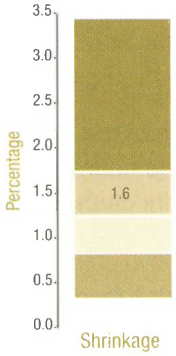
Based on this risk assessment, Mr. Timewell and Ms. Karran develop preliminary positions on the risk response. These determinations are key inputs into determining required control activities.

Example: **Using Benchmark Data to Assess Significance and Response to Risk**

A pet food retailer, Best Bits, uses benchmarking techniques to assess losses in physical inventory from theft. The "shrink percentage" calculated is defined as the value of lost physical inventory divided by net sales. The amount of physical loss is determined through a physical inventory count process.

The company is currently examining ways to enhance its risk response decisions to reduce the significance of the risk by altering either likelihood or impact. Given the company's current level of losses (1.6%), accepting the risk would not be acceptable, and management elects to implement control activities that reduce the likelihood of losses and can detect losses sooner.

Best Bits management also notes the level of losses other companies incur due to shrinkage. The figure below shows the shrinkage for several other similar companies within a benchmark group. Best Bits' losses are noted underneath for comparison.



Quartile 4	1.80%–3.50%
Quartile 3	1.30%–1.80%
Quartile 2	0.88%–1.30%
Quartile 1	0.33%–0.88%

Best Bits	Other Companies		
Average	Low	Median	High
1.60%	0.33%	1.30%	3.50%

Using the data provided in this analysis, management believes that a loss rate target of 1.3% is suitable for the company (e.g., top of quartile 2) and additional control activities are developed within the receiving and shipping process (as part of the Control Activities component). Further, management accelerates the frequency of physical inventory counts to quarterly to improve the accuracy of financial reporting.

Approach: **Considering Internal and External Factors**

Includes Entity, Division, Operating Unit, and Functional Levels

- Analyzes Internal and External Factors

Involves Appropriate Levels of Management

- Estimates Significance of Risks Identified

Determines How to Respond to Risks

Management considers external factors that may impact the ability to achieve financial reporting objectives, such as:

- Economic changes
- Natural or human-caused catastrophes or environmental changes
- New standards
- Changes to laws and regulations
- Changing customer demands
- Technological developments

Management considers internal factors that may impact the entity's ability to achieve its financial reporting objectives, such as:

- Use of capital resource determinations
- Change in management responsibilities
- Personnel hiring and training considerations
- Employee accessibility to assets
- Internal information technology changes

Where these factors are noted, management also considers—in conjunction with the Information and Communication principles—whether some form of internal and/or external communications are needed.

Example: **Analyzing Risks from External Factors**

As CEO of global technology company World Find, Derek Burtnyk makes time for a quarterly discussion on emerging financial accounting standards with each of the company's regional controllers. These discussions focus on potential and announced changes occurring within each jurisdiction, and whether these would require changes to the company's technology systems.

Based on the insights gathered from those discussions, Mr. Burtnyk provides feedback to the various department leaders of World Find. In turn, the department heads use this information to identify additional information requirements and potential technology changes.

In one instance, World Find determined that the accounting requirements for a new value-added tax in one jurisdiction could impact operations in that jurisdiction as well

as two other jurisdictions that interact with it. Based on this assessment, management commenced a project to further refine the assessment of the risks related to the accounting of the new commodity tax, which then served as a basis for how to respond to those specific risks.

Example: **Considering Changes in Information Systems**

Paula Wing is the CEO of a specialty resin company with operations in nine countries. She continually reviews risks to the company by leading monthly staff meetings at which she asks senior managers to comment on any new risks identified, including those related to changes in systems, personnel processes, or activities. Ms. Wong discusses any insights she has on risks facing the company, including those that impact financial reporting. As a team, Ms. Wong and the senior managers develop the needed risk responses.

Approach: **Evaluating Risk Responses**

Management considers a variety of risk responses—avoid, accept, reduce, share—when evaluating whether risks are reduced to an acceptable level. In this process, management may consider unique risks related to financial reporting or a combination of risks. Management may also consider how risk responses impacting the five components of internal control interact to reduce risk to an acceptable level.

- Includes Entity, Division, Operating Unit, and Functional Levels
- Analyzes Internal and External Factors
- Involves Appropriate Levels of Management
- Estimates Significance of Risks Identified
- **Determines How to Respond to Risks**

Example: **Considering Risk Response in a Revenue Process**

Bailey Campbell, the controller for Center Bay Packaging, assesses the risk relating to completeness of revenue. The company has grown over the past five years and now has annual revenues in excess of $50 million. Currently, Center Bay relies on a paper-based bill-of-lading system. Delivery is deemed to have occurred when the bill of lading is signed by the customer as evidence that the goods have been received.

Ms. Campbell has noted instances in the past year where shipping documentation was not provided to the finance department in a timely manner, sometimes as late as two weeks after the shipment was completed. These delays have resulted in misstatement of revenue. Ms. Campbell has determined that the risk related to revenue completeness needs to be further reduced, and so she has decided to implement a bar-code scanner shipping system to track and capture shipments and revenue.

Assesses Fraud Risk

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

Points of Focus

The following points of focus highlight important characteristics relating to this principle:

- Considers Various Types of Fraud—The assessment of fraud risk considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.
- Assesses Incentive and Pressures—The assessment of fraud risk considers incentives and pressures.
- Assesses Opportunities—The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering of the entity's reporting records, or to 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.

Approaches and Examples for Applying the Principle

Approach: **Conducting Fraud Risk Assessments**

- Considers Various Types of Fraud
  Assesses Incentive and Pressures
- Assesses Opportunities
- Assesses Attitudes and Rationalizations

Management conducts a comprehensive fraud risk assessment to identify the various ways that fraud and misconduct can occur, considering:

- The degree of estimates and judgments in external financial reporting
- Methodology for recording and calculating certain accounts (e.g., inventory)
- Fraud schemes and scenarios that are 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
- Last-minute transactions
- Vulnerability to management override and potential schemes to circumvent existing control activities

From these considerations, management makes an informed assessment of specific areas where fraud might exist and the likelihood of their occurrence and potential impact.

Example: **Assessing Fraud Risk**

David Kates, the chief compliance officer at a global retail operation, annually conducts a fraud risk assessment. In doing so, he interviews management at all the international locations about fraud issues. He analyzes:

- Historical fraud activities, including theft of inventory and the processes in place to identify and record such theft
- The methodology used for recording and calculating inventory and shrinkage
- Whistle-blower reports
- The number of manual entries versus automated entries recorded
- The number of late entries due to subjective estimates

With this information, Mr. Kates forms a preliminary view of the potential fraud activities, which he discusses with management of each jurisdiction in order to consider implications and what control activities can reduce the risk of fraud. He also has discussions with human resources personnel and reviews information in the staff files. He uses his historical knowledge and staff information to assess the attitude of the local management toward the tolerance of fraud and to determine whether local management may rationalize fraudulent activities, including corruption.

After completing his fraud risk assessment, Mr. Kates submits a report to the audit committee for its consideration in management oversight.

Approach: **Considering Approaches to Circumvent or Override Controls**

- Considers Various Types of Fraud
  Assesses Incentive and Pressures
- Assesses Opportunities
  Assesses Attitudes and Rationalizations

In identifying and evaluating the presence of entity-wide controls that address fraud, management considers how individuals might circumvent or override controls intended to prevent or detect fraud. Entity personnel, including management, may intentionally override in a number of ways, which may include:

- Recording fictitious business events or transactions
- Changing the timing of recognition of legitimate transactions (particularly those recorded close to the end of an accounting period)
- Establishing or reversing reserves to manipulate results
- Altering records and terms related to significant or unusual transactions

Example: **Maintaining Oversight**

The audit committee of Marker's Medical Supply Company takes the issue of management override of controls very seriously. Consequently, every quarter the committee reviews the fraud risk assessment process. In doing so, the members of the audit committee:

- Maintain an appropriate level of skepticism
- Discuss management's assessment of fraud risks
- Use the code of conduct to assess financial reporting culture
- Ensure the entity has a robust whistle-blower program
- Develop a broad information and feedback network

In addition, the audit committee asks the chief audit executive about:

- What fraud risks are being monitored by the internal audit team on a periodic or regular basis
- What specific procedures internal audit performs to address management override of internal controls
- Whether anything has occurred that would lead internal audit to change its assessment of the risk of management override of internal controls

With this information in hand, the audit committee discusses with the full board and senior management any concerns that need added management focus.

Approach: **Considering Fraud Risk in the Internal Audit Plan**

- Considers Various Types of Fraud
  Assesses Incentive and Pressures
  Assesses Opportunities
  Assesses Attitudes and Rationalizations

The chief audit executive incorporates results of the fraud risk assessment into the internal audit plan. He or she reviews and confirms that the internal audit plan addresses relevant risks.

Example: **Identifying and Analyzing Risk of Material Omission and Misstatement Due to Fraud**

Divisional controllers at Maxwell's, a 24,000-employee consumer products company with locations in several countries, work with business unit leaders to identify and assess potential fraud risks. These risks are prioritized and categorized into various components, including risks of inventory theft, manipulation of data and bias in the development of accounting estimates, and other potential means of overriding controls. Internal audit reviews the resulting fraud risks and provides its point of view. In addition, the company meets with its external auditor to discuss the fraud risks to determine if there are others that should be under consideration. Business unit management plans responses and then selects and develops controls to mitigate these fraud risks.[15]

Approach: **Reviewing Incentives and Pressures Related to Compensation Programs**

Management considers how personnel may rationalize behavior regarding evaluations, compensation, or employment. The board and management review the entity's compensation programs and performance evaluation process to identify potential incentives and pressures for employees to commit fraud. This review considers how meeting, or not meeting, financial reporting targets potentially impacts an individual's evaluation, compensation, and continued employment.

Considers Various Types of Fraud
• Assesses Incentive and Pressures
Assesses Opportunities
Assesses Attitudes and Rationalizations

Example: **Analyzing Compensation Structure**

The compensation committee of the board of directors of Schmidt Auto, a global automotive supplier, annually reviews the executive officer compensation packages with the audit committee, chairperson, and chief auditor. To determine the incentives to management, the following items are discussed:

- Thresholds for significant changes in compensation
- Mix of total compensation versus incentive compensation
- Structure of compensation compared with industry peers
- Mix of long-term compensation compared with short-term incentives

After these discussions for Schmidt Auto's last fiscal year, the board determined that the CFO's incentive compensation, 80% of which was based on the current year's net revenue, was too high and focused too much on the short term. The compensation committee subsequently reduced the incentive compensation, with 40% derived from current year's net revenue.

15 This example is continued in Chapter 6, Monitoring Activities, to illustrate how monitoring activities may assess whether controls to effect principles in the risk assessment are deployed as intended (see page 149).

Identifies and Analyzes Significant Change

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

Points of Focus

The following points of focus highlight important characteristics relating to this principle:

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

Approaches and Examples for Applying the Principle

Approach: **Assessing Change in the External Environment**

- Considers Change in the External Environment
- Assesses Changes to the Business Model
- Assesses Changes in Leadership

Management develops approaches for observing changes in the external market and assessing the potential impact on the entity's operations and financial reporting. This may include reviewing the following:

- Websites and social media
- Website tracking tools
- Newspaper clipping services
- Search engines
- Trade publications and trade shows
- Conferences
- Professional organizations

Example: **Reacting to Significant Change Caused by External Factors**

Last year, Clear Blue Auto Manufacturing became aware of a hurricane approaching one of its off-shore operations that had the potential to cause significant supply disruptions. In response, the company immediately established an internal working team to assess the risks of such a disruption to its manufacturing capabilities, and the risks of its own affected facilities to its overall manufacturing footprint. All significant suppliers were contacted and asked to assess the impact the hurricane might have on their production abilities. A detailed list of parts that might be delayed in production and shipping was created, and then alternative suppliers were identified. Where no alternative suppliers could be found, management identified a prioritization list of which manufacturing location should receive the limited number of parts as they became available.

During this process, the accounting and finance departments of Clear Blue Auto determined how plant shutdowns would affect the financial statements. This included potential penalties contained within various sales contracts, possible obsolescence of parts required for a particular model year being phased out, and greater impacts from extended delays in supply of parts. They also evaluated what insurance coverage was available to mitigate potential losses. These teams were also responsible for identifying incremental risks from required system and process changes when working with the company's suppliers.

The potential impact of this hurricane was updated and communicated to the company's board of directors later that day.

Considers Change in the External Environment
• Assesses Changes to the Business Model
Assesses Changes in Leadership

Approach: **Conducting Risk Assessments Relating to Significant Change**

Following a decision to pursue a new business strategy or significantly change the current strategy, management conducts a detailed risk assessment to consider how the changes might impact the achievement of all objectives set across the entity.

Example: **Updating Risk Assessment for a New CEO**

Geoffrey McPherson was recently appointed the CEO of Garner's Heating, a manufacturer of heating and air conditioning components. One of his first tasks in his new position was to establish a 100-day plan to assess the overall business and determine where changes were required. To initiate the process, Mr. McPherson called a meeting with the leaders of all key functional areas to talk about risk.

Over the next 100 days, Mr. McPherson will be holding individual meetings with each functional team to discuss their current objectives, how those objectives might be changed, and how those changes would impact the assessment of risks to reliable financial reporting. He expects that some at Garner's Heating will be surprised with his proposed changes to policies, which have been largely unchanged for several years. This includes the company's CFO, Ruth Koziak, who is responsible for analyzing the change in strategy and the implications to financial reporting.

At the end of the 100 days, Mr. McPherson intends to reconvene the larger group to discuss how the company should change, and the incremental risks (including financial reporting) that may come with the change. It will then be up to Ms. Koziak and the chief audit executive to consider the implications of the company's new vision and the effects it will have on the external financial reporting objectives.

Example: **Responding to Significant Change from International Exposure**

Consecutive Corp., a multi-billion-dollar technology equipment manufacturer that has historically focused on sales in the United States, has decided to expand internationally with both sales and manufacturing. As part of the expansion plans, Consecutive has assessed several factors:

- Incremental revenue opportunities
- Competition in the marketplace
- Cultural dynamics of the targeted international location
- Different laws and regulations, including those that would affect the company's ability to defend its patents
- Risk of increased fraud from theft and corruption

Each of these factors presents incremental risks to financial reporting and processes that need to be managed. Therefore, Consecutive's corporate controller is performing a risk assessment with the finance teams in the international locations to ensure these new risks are identified and to help management determine how best to respond.

Example: **Responding to Significant Change from an Acquisition**

Industrial products giant Wilson & Zachary recently acquired another multi-billion-dollar company. During the due diligence process, the company performed a risk assessment on the new business and updated its own risk assessment considering the following items:

- New markets that will be encountered by the combined company (including differing financial reporting standards)
- The ability to assimilate the financial reporting processes of the acquired company, including the effects on migrating to a combined information technology system
- The ability to achieve the anticipated synergies from the acquisition and whether these synergies will create incremental risks to financial reporting

A project team has been formed for the transition to ensure that all risks are appropriately identified across all business units and functional areas. Any identified risks are passed on for assessment to senior management, including the company's chief operating officer and chief financial officer.

Approach: **Considering Change through Succession**

As part of the overall succession process, management reviews planned changes in management and leadership positions and the attitudes and values portrayed by the incumbents to those positions through interviews with personnel within the entity.

Considers Change in the External Environment

Assesses Changes to the Business Model

- Assesses Changes in Leadership

Example: **Planning for Executive Transition**

The board of Turnball Insurance annually reviews the transition plans for key executive leadership in the company. As part of this review, the board discusses with the chief audit executive the perceived attitudes and values of those individuals who have been identified as successors. Such considerations may include focusing on attaining profit expectations versus maintaining effective control, including any concerns about the potential management override of controls.

If the transition for a particular position is expected to occur within the next two years, representatives of the audit committee interview the candidates to ensure that their views on internal control are consistent with those expected by the audit committee.

The board considers that feedback attained when making any decisions within the scope of its responsibility. The audit committee communicates its findings to the CEO and other members of senior management, who ultimately will make a decision on successors.

Considers Change in the External Environment
Assesses Changes to the Business Model
• Assesses Changes in Leadership

Approach: **Considering CEO and Senior Executive Changes**

The desired qualities relating to attitudes towards risk, risk tolerance, and internal controls are compiled as part of a comprehensive leadership profile to identify the "ideal" future CEO. This leadership profile is used to evaluate the potential candidates considered for the position. As part of recruiting for the CEO and other executive team members, the audit committee asks candidates to articulate its views on the importance of internal control and how it would balance the need for effective control with other pressures for performance and cost considerations. When assessing the internal candidates, the audit committee also considers the candidates' track record on maintaining control and effectively managing the pressure to perform.

Example: **Preparing for a Change in CEO**

As part of the recent interview process for a new CEO, the board of directors of Mills and Associates, an industrial products company, asked all candidates their perspectives on risk, risk tolerance, and internal control, including current areas of emphasis.

The successful candidate, Jenny Acosta, has a strong background and focus on cost management and streamlining operations. However she agrees with the audit committee that this streamlining could result in fewer processes and controls, especially those viewed to be labor intensive, and that such changes could erode the quality of reporting and increase certain financial reporting risks.

With this in mind, the audit committee has begun to request quarterly updates of controls that have been removed by management and the potential impact on financial reporting. In addition, this information is incorporated by the internal audit group into its internal audit planning process.

4. Control Activities

Chapter Summary

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

Principles relating to the Control Activities component

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

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

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

Principles	Approaches
10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	• Using Matrices, Workshops, or an Inventory of Control Activities to Map Identified Risks to Control Activities • Implementing or Monitoring Control Activities when Outsourcing to a Third Party • Considering the Types of Control Activities • Considering Alternative Control Activities to the Segregation of Duties • Identifying Incompatible Functions
11. The organization selects and develops general control activities over technology to support the achievement of objectives.	• Using Risk and Control Matrices to Document Technology Dependencies • Evaluating End-User Computing • Implementing or Monitoring Control Activities when Outsourcing IT Functions to a Third Party • Configuring the IT Infrastructure to Support Restricted Access and Segregation of Duties • Configuring IT to Support the Complete, Accurate, and Valid Processing of Transactions and Data • Administering Security and Access • Applying a System Development Life Cycle over Packaged Software • Applying a System Development Life Cycle over Software Developed In-House
12. The organization deploys control activities through policies that establish what is expected and in procedures that put policies into action.	• Developing and Documenting Policies and Procedures • Deploying Control Activities through Business Unit or Functional Leaders • Conducting Regular and Ad Hoc Assessments of Control Activities

Selects and Develops Control Activities

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

Points of Focus

The following points of focus highlight important characteristics relating to this principle.

- Integrates with Risk Assessment—Control activities help ensure that risk responses that address and mitigate risks are carried out.
- Considers Entity-Specific Factors—Management considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.
- Determines Relevant Business Processes—Management determines which relevant business processes require control activities.
- Evaluates a Mix of Control Activity Types—Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls.
- Considers at What Level Activities Are Applied—Management considers control activities at various levels in the entity
- Addresses Segregation of Duties—Management segregates incompatible duties, and where such segregation is not practical, selects and develops alternative control activities.

Approaches and Examples for Applying the Principle

Approach: **Using Matrices, Workshops, or an Inventory of Control Activities to Map Identified Risks to Control Activities**

- Integrates with Risk Assessment
- Considers Entity Specific Factors
- Determines Relevant Business Processes

Evaluates a Mix of Control Activity Types

Considers at What Level Activities are Applied

Addresses Segregation of Duties

Once risks have been identified and mapped to relevant financial statements assertions, management determines relevant business processes and selects and develops control activities to address each risk. Management involves relevant stakeholders to identify the appropriate control activities. This includes those individuals responsible for the risks in their areas, finance personnel responsible for financial reporting, and other control experts, such as internal auditors or others who have relevant specialized knowledge. A centralized group responsible for financial reporting or control activities periodically reviews the risk control matrices to help ensure that the entity's financial reporting risks are being addressed.

The selection and development of control activities is achieved through various methods, and may include the following:

- Using matrices to map identified risks to control activities
- Holding workshops to identify appropriate control activities for each identified risk
- Using an inventory of control activities, tailoring them as appropriate

Management considers the segregation of duties and a mix of transaction control activities and business process reviews. Management considers using automated controls whenever the systems in place make it possible. These are supplemented by manual control activities where automated controls are not available.

Example: **Using Workshops to Map Identified Risks to Control Activities**

A multi-million-dollar consumer products company, Prescott International, holds a number of workshops to select and develop appropriate control activities for each identified risk relating to financial statement assertions for revenue recognition. The meetings are attended by employees from various departments—credit, shipping, billing, and customer service—who review the list of activities and link them to risks identified in the company's risk assessment.

After these workshops, Prescott International is able to select and develop policies and procedures appropriate to its business. The controller reviews the matrix of control activities and risks in order to identify any potential risks not previously noted, recommend additional control activities if necessary, and remove unnecessary control activities.

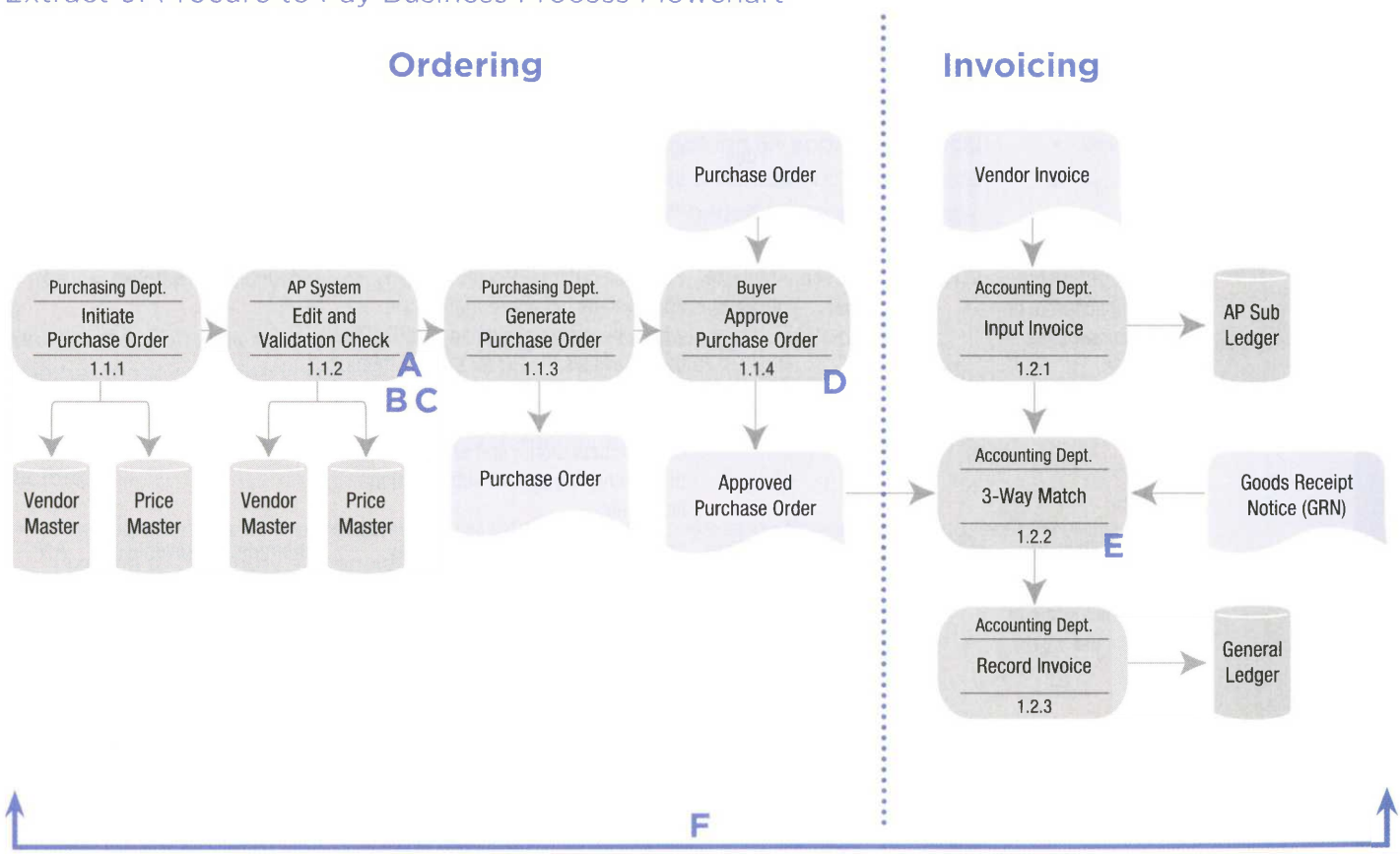
Example: **Using a Risk and Controls Matrix to Map Risks to Control Activities**

A multi-million-dollar manufacturer of sporting goods equipment, Go Rite Sports, develops a matrix in conjunction with its risk assessment process. The matrix sets out:

- Financial reporting objectives and relevant assertions
- Identified risks
- Control activities

Matters such as general ledger maintenance, accruals, management estimates and reserves, period-end close and consolidation procedures, financial statement preparation, and regulatory filings and disclosures are all considered when building the matrix. The risks and controls are described in sufficient detail in the matrix to allow Go Rite's management and others to evaluate whether, if implemented and operating as intended, these actions can sufficiently mitigate the financial reporting risks. As part of this evaluation, management reviews the type of control activity (e.g., preventive versus detective, manual versus automated) to determine if the mix is appropriate. The following illustration is an excerpt of one of Go Rite's risk and control matrices with accompanying flowchart.[16]

Extract of Procure to Pay Business Process Flowchart



16 Note that this is an illustrative matrix and flowchart and does not represent a complete list of all financial risks and control activities in a typical purchasing and payables process.

Extract of Procure to Pay Risk and Controls Matrix

Control	Financial Risk(s)	F/S Assertions (note 1)	Control Level	Frequency of Control	Control Description	Manual/ Automated/ IT Dependent Manual	Preventive/ Detective	Information Processing Objective (note 2)
A	Orders are not accurate	V	Transaction Level	Multiple times per day	During the purchase order (PO) creation the system performs edit checks (auto-populated fields, format checks and use of drop-down lists) of the relevant data fields and auto-populates vendor and item details using the vendor and item master file respectively. The system populates price in the purchase order from the approved master file based on the product entered.	Automated	Preventive	A, V
B	Orders are from an unapproved vendor	E/O	Transaction Level	Multiple times per day	The system blocks POs not using an approved vendor and items from the related master file. Blocked POs are included in the PO exception report that is reviewed daily by the purchasing manager who works with the purchasing agent to either correct or cancel the PO.	Automated	Preventive	A,V
C	Order prices are inaccurate	V	Transaction Level	Multiple times per day	Manually entered PO prices outside those specified in the approved master file must be reviewed and approved in the system by the purchasing manager for processing to continue. Rejected POs are canceled in the system.	Manual	Preventive	A,V
D	Orders are inaccurate or not valid	V, E/O	Transaction Level	Multiple times per day	Purchase orders (POs) must be approved by the appropriate buyer who is in charge of signing the PO. The buyer reviews the PO for various items, including any items out of policy, such as excessive price discounts, inaccurate calculations, and amounts over the purchasing agents authorization limits, etc.	Manual	Preventive	A,V
E	Invoice processing is inaccurate or not valid	V, E/O, R&O	Transaction Level	Multiple times per day	The system performs a three-way match by comparing pertinent data (e.g., price, quantity) between the purchase order, invoice, and receiving document. As part of the three-way match the mathematical accuracy of the incoming invoice is checked. Invoice processing is blocked when differences exceed a predetermined threshold. Blocked invoices are included in the matching exception report that is reviewed daily by the payables manager who investigates and resolves the issue.	Automated	Preventive	A,V

Note 1: E/O = Existence/Occurance; C = Completeness; V = Valuation/Allocation; R&O = Rights and Obligations
Note 2: C = Completeness; A = Accuracy; V = Validity

Example: **Using an Inventory of Risks and Control Activities**

Indigo Brewing is a large global beer brewing company. It has created a standard inventory of risk and control activities that it uses as a basis for all its brewing subsidiaries. It created the inventory by customizing a generic inventory of brewing industry risks and control activities that it obtained from Risk Reverse Inc. with Indigo entity-specific considerations. Some of the entity-specific considerations include:

- Standard company-wide configurations for its enterprise resource planning (ERP) system
- Business performance reviews required of every business unit by corporate finance
- A baseline set of control activities to comply with Sarbanes-Oxley requirements

Following Indigo's recent acquisition of another brewery in China, management used the standard risk and control inventory to develop and select the necessary control activities. It customized this list based on the unique circumstances in the region and to suit the newly merged company, giving the functional leaders responsibility for addressing these risks by implementing control activities in their specific areas.

Approach: **Implementing or Assessing Control Activities when Outsourcing to a Third Party**

- Integrates with Risk Assessment
- Considers Entity Specific Factors
- Determines Relevant Business Processes
- Evaluates a Mix of Control Activity Types
- Considers at What Level Activities are Applied
- Addresses Segregation of Duties

The organization outsources some of its operations to a third party, which may or may not issue a "report on controls at a service organization" following an appropriate local or international standard. Although the organization may rely on an outsourced service provider to conduct processes, policies, and procedures on behalf of the entity, management retains ultimate responsibility for designing, implementing, and conducting an effective and efficient system of internal control.

Management obtains an understanding of the service organization's activities and whether those activities impact significant classes of transactions, accounts, or disclosures in the company's reporting process. In determining the significance of the service organization's processes to the financial statements, the entity considers the following factors:

- The significance of the transactions or information processed by the service organization to the entity's financial statements
- The risk of material omission and misstatement associated with the assertions affected by the processes of the service organization, including whether the activities involve assets that are susceptible to loss or misappropriation
- The nature and complexity of the services provided by the service organization and whether they are highly standardized and used extensively by many organizations or unique and used only by a few
- The extent to which the entity's processes and control activities interact with those of the service organization

- The entity's control activities that are applied to the transactions affected by the service organization's activities
- The terms of the contract between the entity and the service organization, and the degree to which authority is delegated to the service organization

If management determines that the service organization's processes are significant to internal control over external financial reporting, then it:

- Identifies the specific control activities performed by the service organization that are relevant to financial statement assertions, and/or
- Selects and develops control activities internally over the activities performed by the service organization.

If a report on controls at a service organization is available, management can use it to determine what financially significant processes are covered, whether appropriate control activities are in place, and what control activities are required in its own organization to address external financial reporting risks.

If an appropriate report does not exist, management can use the entity's own resources, such as internal audit, to review the control activities and ensure that any external financial reporting risks are mitigated by the combination of its own control activities and those of the service organization.

Example: **Obtaining a Report on Controls at a Service Organization from a Service Payroll Provider**

Green Grow Now is a 250-person company that packages and distributes organic produce. It uses a third-party service, Jennssen Inc., to process payroll, which is considered significant to the company's financial reporting because employee costs are a large part of Green Grow Now's expenses.

Jennssen Inc. engages a service auditor to audit its control activities over transaction initiation, processing, and recording, and to issue an SSAE 16 (SOC1)[17] report on controls. When Green Grow Now obtains the report, it assesses whether the described control objectives and control activities performed by Jennssen impact internal control over external financial reporting related to the existence, completeness, and valuation of payroll expense.

Green Grow Now considers the test results in the report and whether any exceptions have been identified. It also considers the period covered by the report and concludes that it needs additional evidence of the operation of control activities for the period not covered. The management communicates directly with Jennssen to inquire about any changes to its processes; Jennssen confirms in writing that no changes have been made.

Based on this information, Green Grow Now concludes that no further action is needed. It also reviews the control activities that it is expected to have in place in its own organization (as specified by the user control activities in the SSAE 16 report) to verify they are implemented and operating as intended.

17 An independent auditor's report on the design and operating effectiveness of controls at a service organization

Example: **Implementing or Assessing Control Activities when a Report on Controls at a Service Organization is Not Available**

Funnell Medi-Quip is a 500-person medical equipment manufacturer that decides to outsource its treasury function to a service organization, Oxford Financial Experts. A report on control activities is not available.

The management of Funnell Medi-Quip evaluates the nature of the control activities of Oxford Financial Experts and its own control activities over Oxford. The management team determines that the risk of material omission and misstatement associated with the financial statement assertions affected by the processes of the Oxford is high. Funnell Medi-Quip concludes that additional information is needed to evaluate the design and operating effectiveness of Oxford's control activities. The management team performs tests at Oxford, using the internal audit group to verify that the control activities are implemented and operating as intended. Funnell also tests its own user control activities.

Approach: **Considering the Types of Control Activities**

Once risks have been identified and mapped to relevant financial statement assertions, management determines relevant business processes and selects and develops control activities to address each risk. Management considers using automated controls whenever the systems in place make it possible. These are supplemented by manual control activities when automated controls are not available. Management also considers a mix of transaction control activities and business performance reviews. In its selection and development of control activities, management considers the likelihood that a control might fail to operate effectively. In assessing the risk of failure, management assesses various factors, which may include:

- The type of control (i.e., manual or automated) and the frequency with which it operates
- The complexity of the control
- The risk of management override
- The degree of judgment required to operate the control
- The competence of the personnel who perform the control
- Any changes in key personnel who perform the control
- The nature and materiality of misstatements that the control is intended to prevent or detect
- The degree to which the control relies on the effectiveness of other controls (e.g., general technology controls)
- The evidence of the operation of the control from prior years

Certain financial reporting elements, such as those involving significant accounting estimates, related party transactions, or critical accounting policies, will generally have higher risk for both material omission and misstatement to the financial reporting

Integrates with Risk Assessment
Considers Entity Specific Factors
Determines Relevant Business Processes
- Evaluates a Mix of Control Activity Types
- Considers at What Level Activities are Applied

Addresses Segregation of Duties

element and control failure. In these situations a combination of control activities is usually selected and developed by management to adequately address the risks of a financial reporting element.

Example: **Balancing the Types of Control Activities**

During initial compliance efforts, EJ's Corporation faced uncertainty in determining how many controls were needed to achieve management's objectives. Amid such uncertainty duplicate control activities were deployed. EJ's management is re-evaluating its existing controls to:

- Determine whether duplicate control activities can be eliminated
- Identify opportunities to implement preventive control activities earlier in the business process and balance with downstream detective control activities
- Where possible, automate controls and eliminate manual control activities

In balancing its control activities within the processing of journal entries in the financial reporting cycle, EJ's Corporation focuses on the following preventive control activities:

- *Restricted Access*—Ensuring that different people initiate, approve, and record key transactions such as manual journal entries.
- *Authorization, Approval, Verification*—Clearly defining lines of responsibility and expectations with written job descriptions. Setting limits for the authorization of journal entries by job function in excess of a specified limit; controlling access to the general ledger software program through passwords, access codes, and program permission; and requiring a senior-level individual to review supporting documents to verify that journal entries are appropriate, valid, and in agreement with the company's policies.

The following detective control activities complement these control activities:

- *Reconciliation*—Performing regular, independent comparison of different sets of data to identify and investigate any discrepancies
- *Monitoring and Performance Reviews*—Regularly comparing reported results to budgets, forecasts, prior periods, and other benchmarks to identify unexpected results or unusual relationships that require additional follow-up.

Example: **Evaluating Preventive versus Detective Control Activities**

As part of its regular assessment of control activities, Mountain High University reviews the mix of preventive and detective control activities and finds a high proportion of detective control activities. This high proportion of detective control activities is resulting in the processing of transactions to be slow, labor intensive, and error prone as a considerable amount of time is spent fixing errors that occurred earlier in the process. To address the problems management implements more preventive controls earlier in the process, through automated controls, such as edit checks and automated data verification, and review and approval controls at transaction initiation to reduce the number of errors that need to be detected and corrected after transactions are processed.

Example: **Setting the Threshold for Business Performance Reviews**

The senior management of Zephyr Corp., a multinational consumer products company, reviews the monthly and quarterly income statement and balance sheet analysis in order to prevent or detect on a timely basis material omission and misstatements to one or more financial statement assertions. This analysis compares the current year results against prior year actual results, the current year budget, and the latest forecast. It also includes key performance indicators such as gross margin, accounts receivable, inventory turnover days, and return on equity.

To begin the analysis, the CFO of each of the company's five business units reviews the balance sheet and income statement in detail to identify and explain any variances from budget and prior year actual results over a predetermined threshold (which varies by business unit). The threshold, which ranges from 5% to 10% of pre-tax income, has been developed by senior management to help detect potentially material differences considering the following factors:

- Significance of the business unit in relation to the group
- The nature of assets and liabilities and transactions executed at the business unit, including significant transactions or initiatives undertaken outside the normal course of business
- Specific risks associated with the business unit
- Degree of centralization of processes and financial reporting applications
- The effectiveness of the control environment at the business unit
- Results of past monitoring activities by the company
- Potential for error to exist at the business unit

The analysis is then submitted to Zephyr's corporate center for review. Senior management hold monthly meetings with the representatives from each business unit (usually a business unit CFO) to understand why there are significant differences that are exceeding predefined thresholds and to determine whether corrective action is necessary.

Example: **Controlling Significant Accounting Estimates**

Finance management at the Judge Mint Company (JMC) is responsible for preparing accounting estimates relating to the valuation of trade receivables on a monthly and quarterly basis. Management estimates the underlying allowance for uncollectible receivables considering:

- Historical percentages of uncollectible receivables to total receivables
- Historical collections and write-offs relating to customers with specific receivables outstanding at period end
- Judgments relating to customers' ability and intent to pay

Management's assessment of customers' ability and intent to pay outstanding receivables is subjective and susceptible to error. Accordingly, management selects, develops, and deploys a mix of control activities to help mitigate this valuation risk, including the following:

- The treasurer periodically reviews existing customers' historical financial and credit information as provided by Dun & Bradstreet to identify any changes in the customers' ability to pay.
- Automated preventive controls are embedded within JMC's ERP system support generation of sub-ledger reporting, including historical aging, collection, and write-off of receivables by customer, which provides a level of consistency for the completeness and accuracy of reporting used in making estimates.
- Specific adjustments proposed by accounting personnel who are knowledgeable about customers must be supported by analyses including reasons for such adjustments (e.g., communications, disputes, payments, write-offs).
- The assistant controller approves proposed adjustments to the calculated preliminary estimate for specific uncollectible receivables based on review of supporting analyses and information.
- The controller assesses the reasonableness of the final estimate by reviewing the rationale supporting the selection of the historical percentage used to calculate the preliminary estimate and the rationale supporting any material adjustments, and considering the consistency with her knowledge of industry, business, and customer trends/events.

Example: **Automating Balance Sheet Reconciliations**

Gentry Co., a large decentralized industrial products company, has identified the account reconciliations part of the financial reporting process as a critical control activity for reducing the risk of material omission and misstatement in the financial statements. The number of accounts in the company's books has increased significantly over the years as new processes and transactions have been added, other entities have been formed or acquired, and the number of employees has grown. Today, a large volume of accounts are reconciled manually on a monthly basis, but this is a time-consuming process that is prone to error.

Gentry Co. is considering implementing account reconciliation software, which would help automate the process and allow Jeremy Brewster, who is responsible for the process, to spend more time on the more subjective and complex areas of account reconciliation.

Gentry has identified the following benefits that would arise out of using an automated account reconciliation tool:

- A continuous controls monitoring framework would be able to identify significant and material reconciling items, allowing management to quickly respond to potential issues.
- Adjusting entries would be identified and efficiently recorded, followed by a review by Mr. Brewster.
- Labor and cost would be reduced.
- Automation would integrate seamlessly with ledgers, sub-ledgers, and other financial systems.

- Exception management would reduce exposure to risk by establishing an action plan for all exception items.
- Reconciliation processes would be integrated into the email system, automating workflow.

Gentry Co. decides to implement a partial automated process. It uses both qualitative and quantitative factors to determine which reconciliations will be automated and which will continue to be manual. The factors considered favorable to automation include low complexity of transactions, absence of significant judgments and estimates, low number of manual journal entries and adjustments, low susceptibility of transactions to fraud, and high-volume, low-dollar value of transactions, combined with low degree of variation against the expected account balance.

Approach: **Considering Alternative Control Activities to the Segregation of Duties**

Where resource or other constraints compromise the ability to appropriately segregate duties, management considers alternative control activities, such as timely periodic management reviews of reports that are prepared in sufficient detail for misstatements to be identified.

Integrates with Risk Assessment
Considers Entity Specific Factors
Determines Relevant Business Processes
Evaluates a Mix of Control Activity Types
Considers at What Level Activities are Applied
• Addresses Segregation of Duties

Example: **Using Alternative Control Activities when Access to Purchasing Transactions Are Not Segregated**[18]

Luther Optical is a multi-million-dollar designer, manufacturer, and distributor of consumer and industrial optical products. There are two staff members in the purchasing department, each of whom is authorized to prepare, authorize, and issue purchase orders up to $5,000. Because no one reviews these purchase orders before they are sent to vendors, there is a risk that unintentional errors or intentional fraudulent acts will result in inventory valuation errors, obsolescence, or shortages due to diverted shipments. To reduce this risk to an acceptable level, management relies on a combination of control activities carried out by other staff members. These include, but are not limited to, the following:

- An inventory clerk documents and tracks all inventory levels, reducing the risk of obsolescence.
- An inventory receiving clerk evaluates, documents, and reports to management unusual inventory movement, such as excessive ordering that could lead to obsolescence.
- A payables clerk matches invoices to purchase orders and receiving reports before amounts are paid, reducing the risk of errors resulting from diverted shipments.
- A controller reviews exception reports of all inventory purchases with a price more than 10% above current average costing.

18 This example is likely to be most relevant for smaller entities or the smaller sub-units of larger entities.

Integrates with Risk Assessment
Considers Entity Specific Factors
Determines Relevant Business Processes
Evaluates a Mix of Control Activity Types
Considers at What Level Activities are Applied
• Addresses Segregation of Duties

Approach: **Identifying Incompatible Functions**

Using automated tools, organization charts, process flowcharts, or other means by which activities are documented, management identifies incompatibilities in functions that are needed to appropriately segregate duties. These incompatible functions are considered when developing or revising the policies for granting access to assets and systems. The policies are regularly updated to reflect changing responsibilities and activities.

Example: **Manually Assessing Incompatible Functions Across an Entity**

Finansis Corporation is a manufacturer of bicycles that recently implemented an enterprise resource planning system but continues to use its legacy procurement application. Management has identified a risk that personnel perform incompatible functions across the entity's financial reporting systems, and in turn, have inappropriate access to those systems. The CFO, Steve Wu, has formed a task force of representatives from finance, accounting, operations, internal audit, compliance, and IT to review process flowcharts and procedure manuals and to assess the financial reporting risks of the same person being able to perform two incompatible functions (e.g., bill creation and payments). The task force has now created a matrix of incompatible functions across the financial reporting processes and assessed any business justification for the incompatibility. If the business justification is deemed valid, the task force evaluates the sufficiency of alternative controls selected, developed, and deployed. If the justification is found not valid or not existing, the task force develops a recommendation for the controller to implement a policy for segregating the functions.

Senior finance, operations, IT, internal audit, and compliance management have reviewed and approved the task force's recommendations. Commensurate with the policy changes, IT has updated access rights across the various systems. Control activities were selected and deployed to help ensure that the segregation of duties is maintained, including policies and procedures for user management and IT's review and approval of access requests. The policies also include the segregation of duties as criteria in the annual review of access rights performed by user management for each financial reporting relevant system.

Example: **Using Automated Tools to Enforce the Segregation of Incompatible Functions**

Frencorp is a multi-billion-dollar public industrial products manufacturer. Recently it installed and configured a governance, risk, and compliance access management application. The purpose is to assess sensitive access and segregation-of-duty risks and conflicts during the development of security roles and the assignment of those roles to end users. The application allows Frencorp to define processes and transactions that should not be combined in a security role or assigned to the same end user. It prevents the assignment of any access that is deemed incompatible.

Furthermore, the application routinely scans security roles and end-user access, generates reports of access risks and conflicts, and routes the reports to the appropriate people for review. If a user requires access to conflicting transactions, the application recommends a mitigating control activity. Frencorp management's review of the access risks and conflicts reports and mitigating control activity decisions are logged in the application.

Selects and Develops General Controls over Technology

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

Points of Focus

The following points of focus highlight important characteristics relating to the principle:

- 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.

Approaches and Examples for Applying the Principle

Approach: **Using Risk and Control Matrices to Document Technology Dependencies**

- Determines Dependency between the Use of Technology in Business Processes and Technology General Controls
- Establishes Relevant Technology Infrastructure Control Activities
- Establishes Relevant Security Management Process Control Activities
- Establishes Relevant Technology Acquisition, Development and Maintenance Process Control Activities

Management documents the underlying technology that supports control activities in risk and control matrices, flow charts, or narratives. Using this information, management can document the linkage between control activities and technology. Management should understand which aspects of technology (infrastructure, security, technology acquisition, development, and maintenance processes) are important to the continued, proper operation of the technology and any associated automated controls. Management also develops an understanding of how various applications and technologies interface with each other.

Example: **Using a Walkthrough to Understand Technology Dependencies**

A global publicly traded information services organization, Signal Corp., recently acquired a privately held newspaper chain. During the due diligence process, Signal Corp. determined that the management of the newspaper chain did not have a good understanding of which applications were critical to the integrity and reliability of its financial information. To assess this linkage, the internal audit department of Signal Corp. performed a walkthrough of each of the newspaper chain's significant financial processes and documented in a process flow diagram all the applications that supported these processes. These included the automated controls and any controls that depended on system-generated reports.

The walkthrough covered each major class of transactions. The internal audit team asked the relevant personnel of the newspaper chain about all significant aspects of the process.

Approach: **Evaluating End-User Computing**

- Determines Dependency between the Use of Technology in Business Processes and Technology General Controls
- Establishes Relevant Technology Infrastructure Control Activities
- Establishes Relevant Security Management Process Control Activities
- Establishes Relevant Technology Acquisition, Development and Maintenance Process Control Activities

Management understands the use of end-user computing, which includes spreadsheets, that supports its financially significant processes and associated control activities. Management assesses the risks of a misstatement resulting from an error in one of these end-user computing applications. Based on the level of risk, management selects and develops general control activities over the technology covering the relevant processes over:

- Technology infrastructure
- Security management
- End-user computing development and maintenance
- Completeness and accuracy controls between the end-user computing system and other systems

For high-risk end-user computing applications, management considers converting to an IT-supported application.

Example: **Evaluating Financial Close End-User Spreadsheet Control Activities**

Smythe & Smythe International recently evaluated the use of spreadsheets in its financial close process. In doing so, it identified that the spreadsheets supporting the calculation of LIFO (last-in, first-out) adjustment and the fair values of goodwill, intangible assets, and debt were of high risk, based on their susceptibility to error and significance to the financial statements.

Smythe & Smythe also classified the spreadsheets as high in complexity because they included the use of macros and multiple supporting spreadsheets to which cells and values were interlinked. The spreadsheets were used either as the basis for journal entries into the general ledger (LIFO reserve) or as financial statement disclosures (fair value of goodwill, intangible assets, and debt).

The company considered the security, maintenance, and update risks of the spreadsheets and then selected and developed the following control activities:[19]

- *Input Control*—Input data is reconciled to source documentation to cover its completeness and accuracy.
- *Access Control*—File-level access to the spreadsheets on a central server is limited to approved users, and a password is required to access the LIFO reserve spreadsheet.
- *Version Control*—Standard naming conventions and directory structures are in place so only current and approved versions of the spreadsheets are used.
- *Calculation Testing*—When changes to formulas are made they are tested against a manual calculation for accuracy. All spreadsheet formulas are checked for accuracy at least once a year.
- *Overall Analytics*—Analytical business process reviews using pre-established thresholds based on operating income and working capital function as a detective control to find errors in any of the spreadsheets.

Approach: **Implementing or Assessing Control Activities when Outsourcing IT Functions to a Third Party**

Management outsources certain aspects of its IT infrastructure to an outside service provider, which may or may not have a "report on controls at a service organization" following an appropriate local or international standard. If a report is available, management uses it to determine what financially significant IT processes are covered, whether appropriate controls are in place at the service organization, and what controls are required in its own organization to mitigate risks to external financial reporting to an acceptable level.

- Determines Dependency between the Use of Technology in Business Processes and Technology General Controls
- Establishes Relevant Technology Infrastructure Control Activities
- Establishes Relevant Security Management Process Control Activities
- Establishes Relevant Technology Acquisition, Development and Maintenance Process Control Activities

19 Note that not all these control activities are technology general controls only. The first and last bullets could be considered business process–level controls; however the entire list is included to illustrate a more complete consideration of spreadsheets.

If an appropriate report does not exist, management uses internal resources (e.g., internal audit) to review the controls at the third party, verifying that the combination of the company's controls and those at the service organization mitigate risks to external financial reporting to an acceptable level.

Example: **Obtaining a Report on Controls at a Service Organization from a Cloud-Based Service Provider**

E-Book Frontier, a retailer of electronic books, has outsourced its enterprise resource planning (ERP) application to a cloud-based service provider (CSP). To prepare for its initial public offering, the company began to develop and implement a system of internal control in support of its anticipated external financial reporting objectives. E-Book Frontier uses the ERP application to support its revenue, inventory, purchasing, and payables processes, so it supports a number of financial statement line items and their associated assertions.

To that end, the management of E-Book Frontier assessed the risks associated with the business processes outsourced to the ERP cloud service provider and determined a number of control activities and information requirements that needed to be addressed. E-Book Frontier management obtained a Statement on Standards for Attestation Engagements (SSAE) No. 16 (SOC 1) report on internal controls prepared by a third-party service auditor. As part of developing and deploying internal controls across the end-to-end business processes managed in part by the CSP, E-Book Frontier incorporated the review of the audit report as a control activity. In performing its review, management noted the following:

- The scope of the report included certain application controls and technology general controls that were evaluated for both design and operating effectiveness. The controls relating to the customized configuration for the organization were not addressed in the service auditor's report. Management evaluated the impacted business process and related financial reporting risks and selected and developed additional actions and control activities to address these risks.
- The tests of controls covered a time period that correlated with ten months of the company's fiscal year, resulting in a gap of the last two months. Based on management's analysis on the relevance and risk of the related controls, E-Book Frontier determined that corroborative inquiry with the CSP would be adequate for the gap period. To evaluate the continued operation of the CSP controls, management interviewed key CSP personnel to assess whether any changes in the controls or known failures had occurred since the date of the report.

Management reviewed the results of the tests of controls and the service auditor's opinion on the operating effectiveness of the controls to determine whether each control objective was achieved. Two exceptions were noted in the report, and management reviewed the additional information related to these that was provided by the CSP in the unaudited portion of the report. They concluded that one exception was not relevant to their organization. For the second exception, additional procedures were needed.

The second exception related to evidence of customer approval of program changes; management evaluated the sufficiency of E-Book Frontier's controls over approval of changes requested to be performed by the CSP. In addition, it requested a report of all changes for the past six months from the CSP and verified that the report of all changes was complete and accurate. It then compared the list of changes and noted no variances from its internal records.

Based on these additional procedures, management concluded that the exceptions did not result in a deficiency of their system of internal control.

Approach: **Configuring the IT Infrastructure to Support Restricted Access and Segregation of Duties**

The applications, databases, operating systems, and networks that support financially significant processes are configured to support restricted access to financial applications and data consistent with the organization's policies and procedures. The configuration includes a means to authenticate users or systems and enforce restricted access, as well as key parameters, such as minimum password length and the aging of passwords.

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

Establishes Relevant Technology Infrastructure Control Activities

- Establishes Relevant Security Management Process Control Activities

Establishes Relevant Technology Acquisition, Development and Maintenance Process Control Activities

Example: **Configuring the IT Infrastructure to Support Restricted Access and Segregation of Duties**

Woodlawn Wireless Telecommunications, which has a number of applications critical to its financial reporting process, was recently cited for poor infrastructure security controls by its internal audit group. Specifically, the setup of key security parameters, such as password length and complexity, was not consistently applied across these applications, and in many cases they were below industry standards for good practices. To correct the situation, Woodlawn developed a four-step approach:

- Create a three-tier risk rating of the importance of an application and its data to the reliability of the financial-reporting process.
- Develop policies for the settings of key security parameters for all financially relevant technology in use at the company for each risk rating level.
- Assess the importance of each application and its associated infrastructure to the reliability of financial reporting and assign it a risk rating.
- Implement procedures to put in place and monitor compliance with the policies for each application consistent with its associated rating.

Approach: **Configuring IT to Support the Complete, Accurate, and Valid Processing of Transactions and Data**

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

- Establishes Relevant Technology Infrastructure Control Activities

Establishes Relevant Security Management Process Control Activities

Establishes Relevant Technology Acquisition, Development and Maintenance Process Control Activities

Management selects and develops control activities so that transaction processing, whether batch or real-time, is complete, accurate, and valid. Processing is actively checked for problems, either through a manual review of system status and logs or by automated programs with alarms. Timely corrective action is taken when problems are identified. Critical financial data and programs are regularly backed up and procedures are in place to completely and accurately do a restore. The restoration process is regularly tested to help ensure the backup and restoration processes work properly.

Example: **Configuring IT to Support the Complete, Accurate, and Valid Processing of Transactions and Data**

In the data center of Sullivan Financial Services, the IT operations staff monitors the batch and real-time processing of applications (including all financially significant applications) for errors using automated software. The scheduling software on the mainframe application checks for various problems with batch jobs, including data errors and programs that don't complete properly or that run out of order. The operators are alerted to any of these issues and alert the appropriate business process owner based on standard documented procedures.

For applications that process in real time, software is also used to automatically monitor for errors, such as incomplete, inaccurate, or invalid record transfers between systems. When a possible error is detected, the software attempts to resend the record without error. If the error persists, an email alert is sent to an operator who corrects the error following standard documented procedures. Financial management is notified of any errors in a weekly report. The weekly report is reviewed to determine if any accounting record adjustments are required due to the system problems. The controller reviews and approves any changes. (Note: this could be considered a process-level control.)

Approach: **Administering Security and Access**

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

Establishes Relevant Technology Infrastructure Control Activities

- Establishes Relevant Security Management Process Control Activities

Establishes Relevant Technology Acquisition, Development and Maintenance Process Control Activities

Financial management establishes policies that define appropriate access rights to be consistent with job functions, including segregation of duties, for financially significant applications and processes. New access requests or changes to access are reviewed against the policy by the functional owner of the IT resource (i.e., application, database, operating system, or network). The owner of the IT resource periodically recertifies access to ensure it is commensurate with policy. Problem reports, such as excessive improper logins, are regularly reviewed, and follow-up actions are taken when issues are identified.

Example: **Establishing Logical Security**

The management team of a compensation and benefits consultancy reviews logical security controls to prevent unauthorized access to its financial reporting systems as follows:

- *User Accounts*—Formal user account setup and maintenance procedures are in place to request, establish, issue, suspend, change, and delete user accounts.

- *Authentication Controls*—Authentication standards establish minimum requirements for password length and a finite number of login attempts. Only unique user IDs are used to promote accountability and auditability.
- *Privileged Accounts*—The use of privileged ("super-user") accounts is limited to two-system and application administrators who are responsible for IT security management and therefore deemed appropriate. These accounts are monitored by management for improper use.
- *Application Reviews*—The configuration settings for who has access to data related to critical applications and systems are periodically reviewed. Any violations detected are reported to management and corrective action is taken.
- *Security Reviews*—Applications and systems generate security logs, enabling user activity to be monitored and security violations to be reported to management.

Approach: **Applying a System Development Life Cycle over Packaged Software**

Management considers many factors when selecting new packaged software, including functionality, application controls, security features, and data conversion requirements. Management utilizes competent internal resources or hires a third-party vendor to implement the software, following the organization's requirements.

Management follows a defined change-control process to implement system upgrades or patches. This includes assessing the nature of the upgrade or patch and whether it is appropriate to implement. If deemed appropriate, the patch or upgrade is system and user tested in an environment that mirrors production before being implemented. Key stakeholders, such as the functional users, finance, and IT, sign off on the change before it is implemented. Appropriate documentation is maintained to provide evidence that the changes have been made.

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

Establishes Relevant Technology Infrastructure Control Activities

Establishes Relevant Security Management Process Control Activities

- Establishes Relevant Technology Acquisition, Development and Maintenance Process Control Activities

Example: **Managing Changes to Packaged Software**

FabFun Toys is a manufacturer of plastic toys. For several years it has been using packaged general ledger software, and it has developed a set procedure for managing vendor announcements of software upgrades, which is as follows:

- Obtain a description of the change, the rationale for it, the impact on the company's security environment, and implications for user interfaces.
- Outline steps for a back-out plan should the upgrade not perform as expected.
- Develop a plan to test that the edit and validation rules work properly, desired system functions operate as expected and produce the desired results, undesired processing results are prevented, and existing technical capabilities, including control activities critical to external financial reporting, continue to work properly.
- Execute the tests and document the results.
- Maintain a change control log.
- Obtain approval from financial and operational management and end users of the test results prior to releasing the upgrade into production.

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

Establishes Relevant Technology Infrastructure Control Activities

Establishes Relevant Security Management Process Control Activities

- Establishes Relevant Technology Acquisition, Development and Maintenance Process Control Activities

Approach: **Applying a System Development Life Cycle over Software Developed In-House**

Management follows a full system development life cycle (SDLC) covering problem fixes to major implementations. The SDLC covers a number of process steps and control activities, including the following:

- *Initiation, Authorization, Tracking, and Analysis*—Changes are captured in a change control or development specification. The change's progress is tracked and authorization to proceed is made by the appropriate stakeholders. The possible impact to internal controls over financial reporting is assessed, and changes are approved by relevant financial stakeholders.
- *Design and Construction*—Programming standards are followed during the design phase and procedures are put in place to provide version control.
- *Testing and Quality Assurance*—Testing is performed before going live to check if the change meets the specification and has not caused any unintended changes to the existing software. The amount and type of testing varies based on the nature of the change (size, complexity, etc.) and includes unit, system, integration, and user acceptance testing, as appropriate.
- *Data Conversion*—When applicable, data is converted completely, accurately, and validly from the previous technology.
- *Program Implementation and Go-Live Authorization*—The change is approved by the relevant stakeholders before going live, and only the approved version of the software is implemented.
- *Documentation and Training*—End-user and IT support documentation and training are created and updated as needed.

Example: **Managing Changes to Custom Software**

Summer Run Co. provides material-based solutions for electronic, acoustical, thermal, and coated metal applications. IT has recently decided to significantly modify inventory management software, which is considered a financially significant application. To do so, the company must rely on the only two developers on staff to develop, test, and migrate the software to production.

Because Summer Run does not have an automated code promotion utility to control versions and migrations to the production environment, the IT manager, James Robb, takes the following steps:

- Identifies and analyzes risk resulting from the required changes
- Assigns changes to developers so that each works on specific tasks only
- Assigns to the developer not working on a particular change the responsibility for testing the change and migration to production
- Reviews any significant changes
- Locks versions following user acceptance testing to prohibit further change prior to release

Mr. Robb also relies on these manual controls to manage the code version and migration:

- Creating a manual log listing the version of the code copied to the development environment, along with date and time, and manually tracking the migration to test and then to production.
- Separating the review of all version control procedures prior to moving the code to production from those performed by the individual responsible for the IT functions.

Example: **Varying Control Activities in an SDLC Based on Risk**

The multi-billion-dollar telecommunications organization, Brassen Systems, uses an SDLC to update and maintain more than 200 applications. The changes vary from large and complex development initiatives to simple report changes. Brassen seeks to match the degree and rigor of control activities to the range of risks of these changes.

The organization assigns the level of risk to one of four categories based on several factors, including the length, level of effort, possible risks to financial processing and control activities, and complexity of the change. Level 1 changes (the most risky) are required to go through twenty quality gates, or control points, before implementation, while Level 4 changes (the least risky) are required to go through only ten gates. All changes that may affect financial processing and control activities are required to be reviewed by someone in the finance department before being implemented.

Deploys through Policies and Procedures

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

Points of Focus

The following points of focus highlight important characteristics relating to this principle:

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

Approaches for Applying the Principle

Approach: **Developing and Documenting Policies and Procedures**

Management develops and documents policies and procedures for all significant external financial reporting–related control activities. Procedures are documented using various formats, such as narratives, flowcharts, and control matrices. Management develops a standardized format for policies and procedures, which may include:

- Reasons for the policy and procedure, including the risks to the achievement of management's objectives
- Locations, units, and processes to which the policy and procedure applies
- Roles and responsibilities for owning, creating, implementing, executing, and maintaining the policy and procedure
- Matters covered by the policy and procedure, including corrective action to be taken as part of performing the control activity
- Escalation procedures for policy exceptions
- Cross-references between associated policies and procedures
- Required competency of personnel performing procedures
- Required timeframe for performing procedures
- Review date

- Establishes Policies and Procedures to Support Deployment of Management's Directives
- Establishes Responsibility and Accountability for Executing Policies and Procedures
- Performs in a Timely Manner
- Takes Corrective Action
- Performs Using Competent Personnel
- Reassesses Policies and Procedures

Example: **Using Templates to Document Policies**

Greyson Gas, a natural gas utility, uses a standardized template to format its policies. Its loss contingencies policy helps ensure that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles. The policy includes the following sections:

- *Purpose*—This policy establishes criteria that are to be used to determine if a loss contingency should be recorded in the financial statements.
- *Location and Applicability*—This policy applies worldwide to any unit of any company owned fully or partially, either directly or indirectly through a subsidiary, by the company, whether consolidated or accounted for by the equity method.
- *Key Provisions*—A definition stating what constitutes a contingency is included and related accounting model is described.
- *Roles and Responsibilities*—Descriptions are provided for everyone involved in the loss contingencies identification, accounting, and disclosure process including the timeframe for completion. This includes each location's senior financial executive notifying the group's senior financial executive and the corporate controller of the existence of an actual or potential loss contingency, including the facts and circumstances giving rise to the possible loss and the estimated amount of such loss. Existing actual and potential loss contingencies are reviewed and evaluated on an ongoing basis (not less than once each calendar quarter) by each location's senior financial executive. As a part of this review, the current status, including

revised estimates for each loss contingency, is reported to the corporate controller. Information required for the disclosure of loss contingencies is provided to the corporate office by location in quarterly financial/legal reporting in a prescribed template. The template is updated, as necessary, through and including the date of the related public filing.

- *Escalation Procedure for Exceptions*—All instances of identified non-compliance with accounting policy must be referred to the corporate controller and the appropriate business unit CFO. All accounting policy exception requests must be referred to the appropriate business unit CFO for preliminary approval, and then submitted to the corporate controller for final approval.
- *Review Date*—The policy is reviewed every two years or when circumstances change for compliance with certain criteria, such as legal and regulatory requirements; applicable rules and regulations; relevance; and appropriateness in supporting business objectives.

A record of all accounting policy changes, additions, and retirements is maintained, which includes revision number and date, effective date, a brief description of the changes made, and the person who approved the change.

Example: **Establishing Policies and Procedures**

A national trade association establishes a policy that all payments must be appropriately authorized before cash is remitted. It uses an authorization approval matrix for expenditures.

The board of directors reviews and approves the annual budget, over and above the required approval provided by the CEO. Authorization to incur liabilities on behalf of the trade association is limited if they fall outside of the amounts approved in the budgeting process for normal operations. The limits are:

- Board of directors: $50,000 or more
- CEO: Up to $50,000
- Vice-presidents: Up to $10,000
- Staff directors and managers: Up to $2,500
- Supervisors: Up to $500

Siobhan O'Reily, the association CEO, must review and approve in writing any capitalized purchases above $10,000. A purchase order must be prepared for all purchases, and every disbursement of funds requires the receipt of an invoice. This policy does not apply to the purchase of association investments, which are authorized by the board of directors through its corporate investment policy.

Ms. O'Reily reviews all purchase orders for more than $10,000 for appropriateness. She compares the amounts to budget, and if she uncovers a discrepancy, she sends the purchase order back for investigation and follow-up.

Example: **Establishing Responsibilities for Reviewing Financial Statements**

Good Chip Company, a public company in the US that manufacturers microchips, issues interim and annual financial statements. As part of the entity's policies and procedures relating to its financial reporting process, responsibilities for reviewing the financial statements are established. Abby Champion, chief financial officer, Alex Pender, controller, and the disclosure compliance committee have separate responsibilities for reviewing draft financial statements before issuance.

Mr. Pender is responsible for reviewing initial draft financial statements (initial draft) along with the corporate financial reporting package, which was prepared by Jayden Roberts, director of financial reporting with input from Jack Jones, director of tax. Mr. Pender's responsibilities include:

- Reviewing reconciliations to trial balances, other accounting records, and analyses to ascertain that the initial draft has been prepared in accordance with policies set forth in the corporate financial reporting manual
- Reviewing the completed financial reporting checklist (which is periodically updated for changes in financial reporting rules and standards) to ascertain that material presentations and disclosures have been prepared in accordance with Generally Accepted Accounting Principles
- Reviewing internal financial reports prepared by controllers of operating units that are expected to identify any material (or unusual) transactions and events that require judgment in presentation and disclosure (For these transactions or events, Mr. Pender inquires of controllers and/or examines supporting records and analyses to concur or challenge the proposed presentation and disclosure.)
- Reviewing comments on initial draft provided by operating unit managers, treasurer, director of tax, and others to identify any other financial reporting matters that require resolution
- Completing his review, updating initial draft, and submitting the final draft and summary of any matters, which require resolution by senior management, to both Ms. Champion and the disclosure compliance committee

Ms. Champion is responsible for reviewing the final draft and summary of matters that require resolution. Her responsibilities are:

- Asking Mr. Pender about the results of his review procedures and summary of matters requiring resolution of senior management
- Reading the final draft to identify any potential material misstatement (or omission) in presentations and disclosures of business conditions, significant transactions, and events
- Evaluating proposed resolutions of specific presentation and disclosure matters and considering which issues to escalate for discussion and concurrence by the disclosure compliance committee
- Approving the financial statements following completion of review by the disclosure compliance committee

- Presenting financial statements and summary results of significant accounting and financial reporting matters to the chief executive officer and audit committee for their review and approval

The disclosure compliance committee comprises the chief operating officer, chief financial officer, chief compliance officer, chief audit executive, vice-president of research and development, vice-president of supply chain, controller, vice-president of tax, and general counsel. The committee members review the final draft. Responsibilities of committee members are:

- Inquiring about the results of both Ms. Champion's and Mr. Pender's review procedures
- Reviewing all information to be published and its draft wording
- Concurring with proposed resolutions of specific presentation and disclosure matters or remanding matters to functional management for further research and recommendation for resolution
- Overseeing disclosure procedures and coordinating disclosures to external parties (shareholders, market authorities, investors, the press, etc.)
- Informing the chief executive officer and chief financial officer of any changes, deficiencies, or material weaknesses pointed out by the disclosure compliance committee

Example: **Reassessing Policies and Procedures for Revenue Recognition**

A large multinational software provider revised its revenue recognition policy due to the risk that lucrative sales commissions have tempted sales personnel to record software orders improperly. Depending on the nature of the software sale, there are different commissions paid to sales personnel. Also, depending on product code, there are different revenue recognition requirements; some products require revenue recognition at the time of sale whereas others require revenue to be recognized over time. Sales personnel occasionally record sales under the wrong product codes, which leads to inappropriate recognition of revenue and sales commissions.

The CEO and CFO approved modifications to the company's revenue recognition policy and related approval matrix that requires all significant software contracts be reviewed by the CFO and other finance personnel before software revenue and sales commissions are recognized. In addition, finance, legal, and sales personnel collaborated in establishing standard contractual terms and conditions that would result in proper recognition of revenue and commissions, and identifying variances from such standards that would require review and approval by the CFO and/or other finance personnel with appropriate technical competencies in applying the company's revenue recognition policy.

In addition, the CFO, sales executives, and legal staff meet annually with sales personnel to review the company's policies, its standard and non-standard contractual terms and conditions, its historical revenue recognition issues, and any specific commercial arrangements to avoid. All subsidiary sales and finance personnel attend annual training

that focuses on how to comply with local laws and regulations and with the company's revenue recognition policies and procedures.

Example: **Reviewing Cost Overruns by Competent Personnel**

The CFO of Boxtop Construction, Suri Navrat, evaluates the process and control activities for assessing cost overruns. She determines that the project manager, George Whitfield, is critical to the process because he is skilled in understanding client needs and project requirements and in analyzing the effects of the alternatives on the project costs and schedule, and, ultimately, the revenues over the project's lifetime.

Mr. Whitfield periodically reviews actual costs incurred for a long-term project, ensuring they are accurate, that indirect costs are appropriately allocated, and that change orders and potential cost overruns do not exceed the authorized funding. If any variances from the cost baseline appear, he promptly investigates them and excludes incorrect or inappropriate changes from the reported cost or resource usage, which is used as the basis for revenue recognition for the period. He also reviews the estimated costs for reasonableness, taking into account the actual stage of construction at the end of the reporting period.

Example: **Performing Control Activities in a Timely Manner**

A large for-profit educational institution, Learn Now College, promptly deactivates or removes access rights to the general ledger from employees who no longer require them. Several steps are followed in this process:

- When an employee is terminated or transferred, a Termination Personnel Action Form/Employee Clearance Form is completed. This form includes a security section, which is completed by someone in the finance department. This section indicates that an information systems change order has been submitted to delete system access permissions for a particular employee.
- The IT group sends a confirmation to the finance department and human resources when the change order is completed.
- The human resources department maintains a list of open change orders that is reviewed daily for receipt of the confirmation from the IT department. If a receipt is not received within twenty-four hours, a human resources representative follows up with the IT group until the request is processed.

Example: **Taking Corrective Action**

As part of the business performance review process, management of White and Stack Co. reviews the results of its business unit, comparing the actual results for the current three-month period with budgets and prior period actual results. The management team observes any significant shortfall in current results compared with the budget, and any existence of performance-based bonus accrual to be paid out when actual performance exceeds budgeted results. Management follows up on the results of its top-level review, identifying any overstatement in bonus accrual.[20] Corrective action is taken as necessary by adjusting the amount recorded for bonus payouts.

20 Investigation of the root cause of why the overstatement occurred is discussed in Chapter 6, Monitoring Activities.

- Establishes Policies and Procedures to Support Deployment of Management's Directives
- Establishes Responsibility and Accountability for Executing Policies and Procedures

Performs in a Timely Manner

Takes Corrective Action

Performs Using Competent Personnel

Reassesses Policies and Procedures

Approach: **Deploying Control Activities through Business Unit or Functional Leaders**

Business unit or functional leaders deploy control activities in their areas of responsibility by building the policies and procedures into their organization's day-to-day activities. In some cases, a centralized control function or team works with the business unit or functional leaders to help deploy policies and procedures consistently across the organization. The policies and procedures are communicated in various ways, including running training programs, holding meetings, and distributing formal and informal documentation.

Example: **Deploying Control Activities through a Central Control Function**

A federal agency has identified its most significant financial reporting risk as the misclassification of expenditures as capital or expense. As a result, the agency director has mandated far-reaching organizational changes in procedures and control activities.

Budget formulation and execution processes and structures have been redesigned centrally to identify and distinctly categorize funds for capital projects. These have been distributed to individual departments by the financial planning and budgeting group. The standard contract has also been modified to require purchased capital items to be separately identified for each project (by budgetary funding code) and to not include items for any other projects.

The agency has instituted new policies, mandatory annual training, weekly reviews of pending contract actions, and monthly reviews of expenditures to ensure program compliance. The efforts have dramatically reduced misclassifications and overcome audit qualifications for plant, property, and equipment reporting.

Establishes Policies and Procedures to Support Deployment of Management's Directives

Establishes Responsibility and Accountability for Executing Policies and Procedures

Performs in a Timely Manner

Takes Corrective Action

Performs Using Competent Personnel

- Reassesses Policies and Procedures

Approach: **Conducting Regular and Ad Hoc Assessments of Control Activities**

On a regular basis, or when changes are made to financially significant processes and systems, control activity owners in conjunction with financial reporting and control experts review control activity documentation for continued relevance. Changes are made when redundant, obsolete, or ineffective control activities are found.[21]

Example: **Regularly Assessing Policies and Procedures**

Central Community Bank maintains a policy checklist on its intranet. The checklist references all the pertinent company policies and management's last review date, next review date, and board of director review and approval as applicable. The policies and procedures are reviewed annually or more frequently if necessary, in response to changes in underlying business processes. The internal audit department assesses compliance with company policy and procedures in conjunction with its internal audit reviews.

21 This approach applies to changes that are not significant enough to go back through the risk assessment process.

Example: **Ad Hoc Assessing of Control Activities**

Following a finance effectiveness review, Cymbol Creative, a global paper products manufacturer, reduced the number of its business unit accounting groups from six to four, combining accounting for related business operations under one CFO. Following the reorganization, the company reassessed and, in certain instances modified, its control activity policies and procedures to reflect the new organizational structure.

5. Information and Communication

Chapter Summary

Information is necessary for the entity to carry out internal control responsibilities to support the achievement of its objectives. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of 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 internal control.

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

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

Principles	Approaches
13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.	• Creating an Inventory of Information Requirements • Obtaining Information from External Sources • Obtaining Information from Non-Finance Management • Creating and Maintaining Information Repositories • Using an Application to Process Data into Information • Enhancing Information Quality through a Data Governance Program • Identifying, Securing, and Retaining Financial Data and Information
14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	• Communicating Information Regarding External Financial Reporting Objectives and Internal Control • Communicating Internal Control Responsibilities • Developing Guidelines for Communication to the Board of Directors • Reviewing Financial and Internal Control Information with the Board of Directors • Communicating a Whistle-Blower Program to Company Personnel • Communicating through Alternative Reporting Channels • Establishing Cross-Functional and Multi-directional Internal Control Communication Processes and Forums
15. The organization communicates with external parties regarding matters affecting the functioning of internal control.	• Communicating Information to Relevant External Parties • Obtaining Information from Outside Sources • Surveying External Parties • Communicating the Whistle-Blower Program to Outside Parties • Reviewing External Audit Communications

Uses Relevant Information

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

Points of Focus

The following points of focus highlight important characteristics relating to this principle:

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

Approaches and Examples for Applying the Principle

Approach: **Creating an Inventory of Information Requirements**

- Identifies Information Requirements
- Captures Internal and External Sources of Data

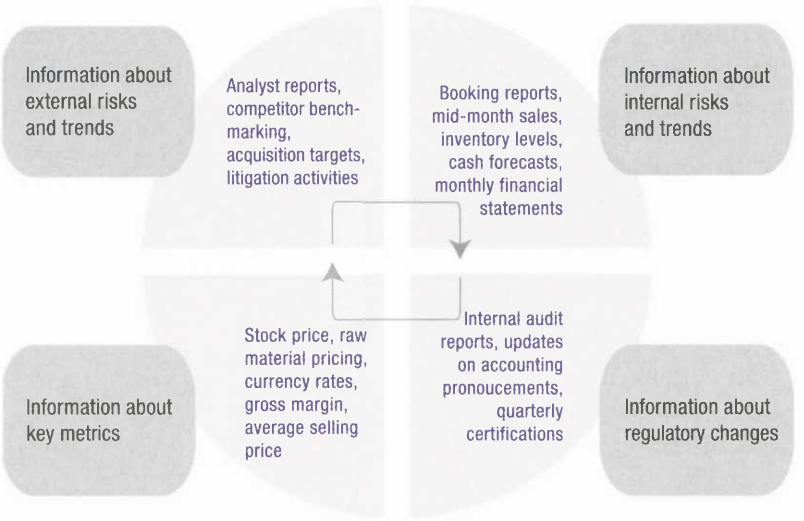
  Processes Relevant Data into Information

  Maintains Quality Throughout Processing
- Considers Costs and Benefits

Extensive information is available to management and comes from a wide variety of sources. For information to be relevant, it must be directly aligned to management's needs and responsibilities for overseeing external financial reporting and monitoring the internal control system. A process for identifying information requirements and building an inventory enables management to focus attention on information that directly supports its needs.

To achieve this, financial management defines common categories and types of information that are aligned to external financial reporting objectives and related risks as specified by management. From these categories, financial management identifies relevant information from both internal and external sources that are best suited to management's needs. Financial management creates an inventory of information and maps each item to one or more members of management that have a role in external financial reporting. This inventory is then used to assign responsibility to personnel for gathering the required information.

The following diagram illustrates key categories and types of information senior management may require in support of external financial reporting objectives:



Example: **Evaluating Business Activities to Identify Information Requirements**

Over the past year, a network of healthcare providers, NetHealth, has experienced significant growth in the number of patient visits. This has created challenges at the medical offices in capturing adequate information for the central processing group. The central processing group relies on adequate information to track and record information on patient visits, which in turn is used to update insurance reimbursement limits and to bill patients and insurance companies.

The management organization overseeing NetHealth recognizes that timely, relevant information is needed to support control activities and keep each physician office in the network up-to-date on patient activities, insurance arrangements, and billing and collection activities. Consequently, the COO has hired an advisor to interview members of the central processing group, receptionists, nurses, doctors, and others who work in physicians' offices across the network. From these interviews, the advisor provided the following:

- Summary of the end-to-end activities of typical patient visits
- Identification of the information requirements to be gathered during each visit
- Definition of roles and responsibilities for information gathering to allow the central processing group to update patient records and process bills accurately and in a more timely fashion
- Identification of data flow challenges that were impacting financial transaction processing and control activities

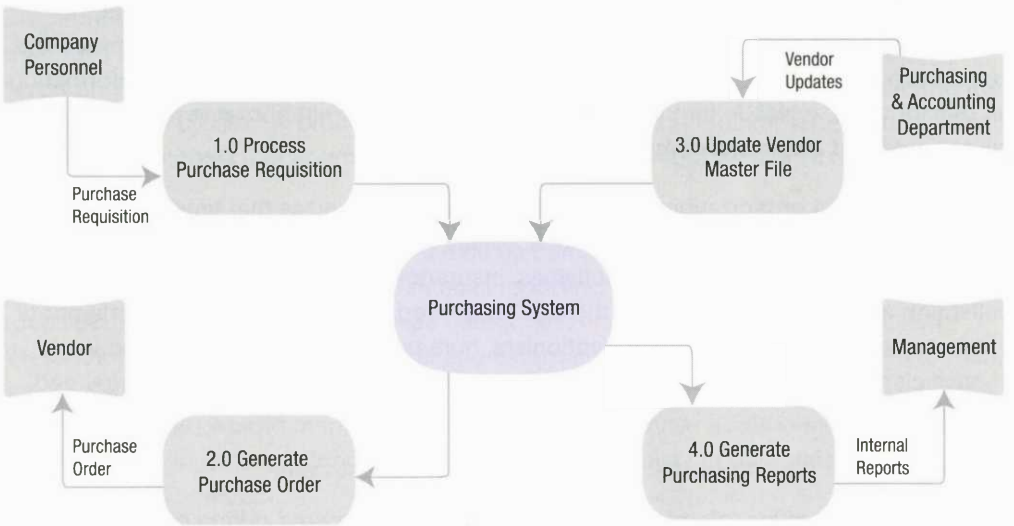
Management is now developing guidelines for gathering information during patient visits. To reduce the costs of distributing the guidelines to each office in the network, the IT manager is building a section on the network's website where the guidelines will be available and where updates and comments can be posted.

Example: **Maintaining Data Flow Diagrams, Flowcharts, Narratives, and Procedures Manuals**

The management at Rahmany Marine Group has effectively adopted the use of narratives, flowcharts, data flow diagrams, and procedures manuals to document the end-to-end process flows that support the corporate internal control and financial reporting. These documents are produced so that information about these processes can be easily understood by users throughout the company, including the IT team, finance and accounting specialists, systems developers, support personnel, and auditors. This documentation allows these personnel and other users to identify the source of data, responsible personnel, storage locations, source systems, relevant transformation processes and quality checks, and the primary users.

The data flow diagram below illustrates part of the company's purchasing cycle. (Note: The following data flow diagram does not depict a complete account of all the information needs for the example. It does depict the flow of information at a high level, but

keep in mind that additional detailed specifics would be included in corresponding narratives, or additional flow diagrams or flowcharts would show a level deeper.)



Approach: **Obtaining Information from External Sources**

Identifies Information Requirements

- Captures Internal and External Sources of Data
- Processes Relevant Data into Information

Maintains Quality Throughout Processing

Considers Costs and Benefits

Finance personnel often rely on publications, events, and other information from external parties to gather information relevant to performing their responsibilities. The sources of data and information vary depending on the specific role and responsibilities of the individual. Sources of information may include:

- Subscriptions to industry publications and regulatory updates
- Participation in industry conferences, trade shows, and other events
- Regular communications, both verbal and electronic, with suppliers, customers, or third-party service providers
- Membership and participation in relevant organizations
- Subscription to third-party mailing lists and social media feeds (e.g., podcasts and blogs) that pertain to the industry and company
- Industry research reports
- Peer industry calls and financial fillings

Finance personnel evaluate the external information gathered and incorporate significant events, trends, and changes into their day-to-day financial reporting or related internal control responsibilities. In addition, finance personnel ensure that any announcements about changes to current accounting standards or regulatory requirements are summarized, reviewed, and disseminated to the others within the external financial reporting organization.

Example: **Gathering Information from External Sources**

J.J. Power Utility Corp. offers a learning and development program that includes guidelines and funding for finance and accounting personnel to attend external training and conferences. These activities help employees achieve their ongoing professional educational requirements, maintain their relevant certifications, and develop new skills. The external training also provides information about new or changed accounting, disclosure, and internal control requirements, as well as best practices important to J.J. Power Utility's business. To supplement the external training sessions, finance and accounting personnel also subscribe to relevant accounting publications.

Accounting and finance personnel meet regularly with the internal audit department to review and update internal accounting and control policies and procedures based on the information gathered. In addition, they meet with the CFO to pass on any new information and to discuss the impact on financial reporting and policies and procedures. Accounting and finance managers update policies and procedures to reflect the impact of the new information.

Example: **Capturing Information through Electronic Data Interchange**

Mandela & Co., a distributor of electronics products, engages in tens of thousands of high-volume, low-dollar transactions with customers and suppliers. Historically, sales orders and invoices for purchasing transactions have been entered and validated through a combination of manual and semi-automated processes.

To reduce time, costs, and errors caused by human intervention, management has implemented electronic data interchange (EDI) to replace the original process. Relevant information about key business transactions is now automatically populated into the company's ERP system, and automated validation checks are in place to confirm that information is transmitted completely and accurately. As well, the information generated through the EDI process is also available to production managers, order management, and billing personnel, which allows them to perform control activities to support proper end-to-end transaction processing, including creating the corresponding accounting entries.

Approach: **Obtaining Information from Non-Finance Management**

External financial reporting objectives are impacted by non-financial activities that occur throughout the business. Information about new events, changes, or significant trends is needed to support accounting, disclosure, and internal control activities. Therefore, senior accounting and finance personnel meet at least monthly with management and personnel in other areas of the business—such as operations, human resources, compliance, and product development. During these meetings, information is gathered verbally and in writing on business events and trends. Topics may include:

- New or lost significant customers, suppliers, or other stakeholders
- Rate and impact of employee turnover

- Identifies Information Requirements
- Captures Internal and External Sources of Data

Processes Relevant Data into Information

- Maintains Quality Throughout Processing

Considers Costs and Benefits

- Unexpected trends, whether negative or positive
- Indications of unethical or improper behavior
- Budget versus actual and forecast expectations
- Contractual, compliance, or regulatory issues
- Customer or supplier complaints
- Findings from internal audit reports

Accounting and finance personnel summarize the information gathered and meet with the appropriate member of senior management to evaluate the impact on the financial statements, internal control effectiveness, or changes needed to policies and procedures.

Example: **Conducting Quarterly Interviews of Operations and Other Management**

Juan Fernandez is the chief accounting officer of Friesens Fresh Foods, a perishable food supplier company. He is responsible for evaluating inventory reserve balances as part of the monthly close process.

Significant changes in purchase commitments, inventory usage trends, product configuration preferences, and cycle count results have impacted the judgments and estimates made in applying the inventory reserves policies. Consequently, Mr. Fernandez now obtains and reviews reports from the company's ERP system to identify unusual or unexpected trends, changes in balances or volumes of transactions, and other relevant details. He then meets monthly with department heads of customer service, procurement, inventory management, and logistics (who oversee third-party warehouses) to collect additional information about customers, products, inventory, and balances.

Based on these meetings, Mr. Fernandez reviews inventory reserve policies, documents key data points that impact prior estimates, and prepares an updated analysis supporting inventory reserve requirements. The CFO of Friesens then reviews and approves the analysis as part of her review of the related journal entries during the month-end closing cycle.

Example: **Obtaining Operating Information for Financial Reporting**

Laccona Electronics, a manufacturer of electrical equipment and components, is responsible for complying with environmental regulations associated with the company's manufacturing processes, including handling raw materials and operating production plants. Laccona's customer contracts include provisions for monetary damages in cases where products are determined to be unsatisfactory as a result of compliance audits performed by environmental agencies. In addition, if the audits are unsatisfactory—that is, they indicate any non-compliance with regulations—Laccona may incur significant fines.

Arlene Gomez, the company controller, obtains monthly reports on operational and compliance metrics from the chief operating officer. In addition, she reviews periodic internal audit reports on the company's adherence to policies and procedures related to

environmental compliance. She uses this information to assess reserve requirements or disclosures associated with damages provisions. Finally, she summarizes relevant information and meets with the CFO quarterly to determine whether changes in accounting estimates and financial statement disclosures are needed.

Approach: **Creating and Maintaining Information Repositories**

- Identifies Information Requirements
- Captures Internal and External Sources of Data
- Processes Relevant Data into Information
- Maintains Quality Throughout Processing
- Considers Costs and Benefits

Senior management establishes a policy for handling information that is gathered, produced, and shared throughout the company. The policy is designed to facilitate the efficient capture, use, and reuse of relevant information supplied to management and personnel across the company.

Management and employees in external financial reporting roles follow procedures for identifying and categorizing information. These procedures require that attributes about each piece of information be recorded before the information is accepted into the repository. The attributes may include:

- Information owner
- Expected users
- Sources (including systems and people)
- Criticality
- Frequency
- Process supported
- Retention period

The information repositories are subject to control activities that help ensure the completeness, accuracy, security, validity, and lack of redundancy of the information.

Example: **Using a Data Warehouse to Facilitate Access to Information**

International Food Distributors has recently completed an enterprise-reporting project to identify and inventory information used across the company for external financial reporting and related internal control. The results of the project were used by the chief information officer and chief financial officer to design a company-wide data warehouse and reporting tools that would support a single source for financially relevant information.

- The first phase of the project involved creating an inventory of the existing reports identifying relevant sources and eliminating non-critical and redundant reports.
- The second phase involved designing and implementing the functional and technical capabilities needed to capture and store data used to generate relevant information. This includes the consideration of automated control activities around completeness, accuracy, restricted access, and validity of the data and information generated.

- The third phase involved training end users on techniques for effective input and extraction of information and reports from the data warehouse using reporting tools.
- The final phase involved designing and implementing operating procedures and control activities over the data warehouse and reporting tools to ensure the completeness, accuracy, restricted access, and validity of the data and information input and reports generated.

As a result of the project, International Food Distributors has a well-defined inventory of reports, improved data, and a more efficient process for capturing and using information for external financial reporting.

Approach: **Using an Application to Process Data into Information**

- Identifies Information Requirements
  - Captures Internal and External Sources of Data
- Processes Relevant Data into Information
- Maintains Quality Throughout Processing
  - Considers Costs and Benefits

Management designs its computer applications to capture data from internal and external sources, transform the data into information, and maintain the quality of the data and information throughout processing and reporting. The activities relating to capturing and processing data about financial transactions (e.g., initiate/enter, authorize, record, process, and report) are documented in company policies and procedures manuals. The application design includes automated application controls such as input checks for existence and validity and output checks for completeness and accuracy. It also is supported by technology general controls.

Example: **Data Capture and Processing for the Purchasing and Payables Cycle**

Insight Media, Inc., a publishing company, recently implemented the purchasing and payables module of its existing ERP system. The key goals were to improve data quality, reduce manual handoffs through automation, and improve information flow and visibility into purchasing transactions.

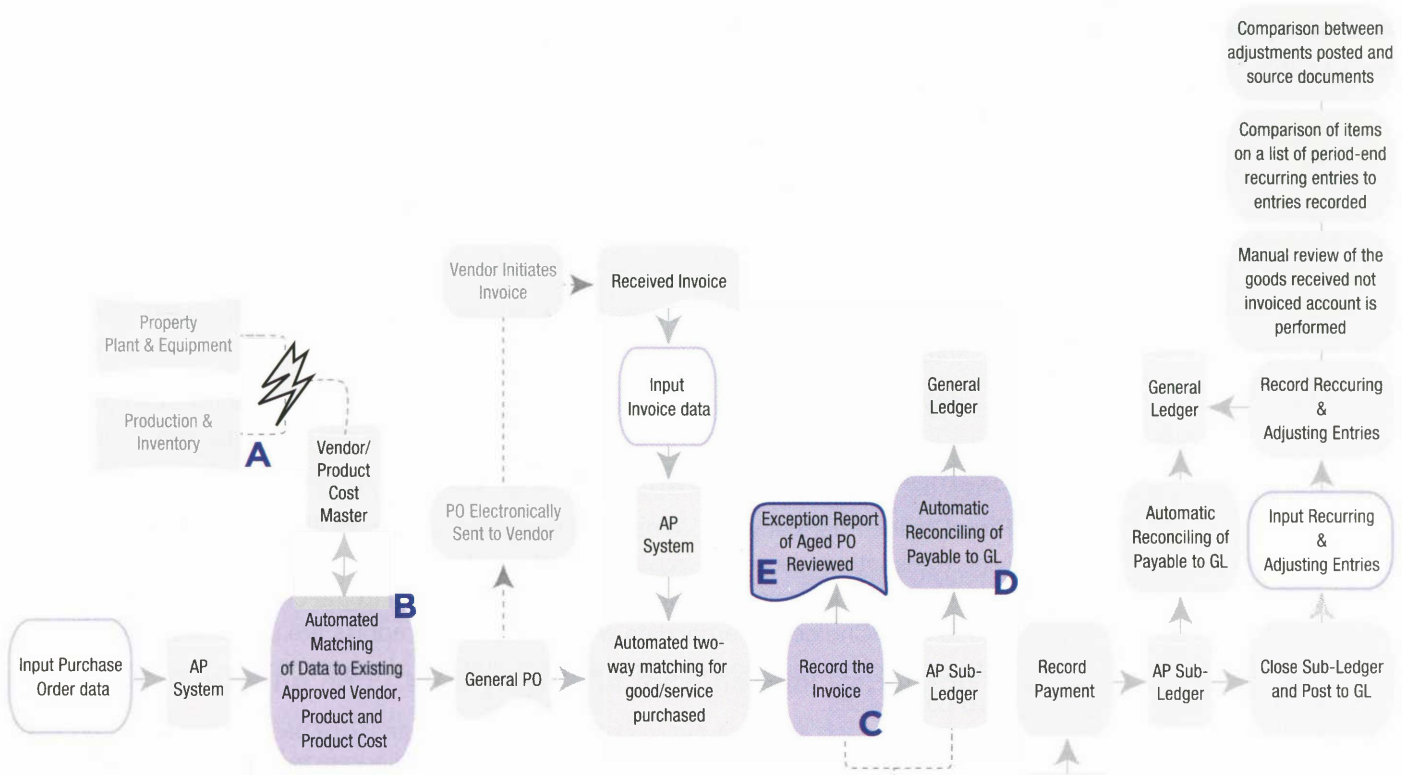
The implementation project team was led by the controller, who was supported by employees involved in the purchase to payables process. Workshops were held to confirm the current end-to-end process and identify important information about sources of transactions, key data requirements, risks to financial reporting, and information required for accounting and reporting. The project team used the results from these workshops to review the ERP module's capabilities for automating tasks and controls such as:

- Checking that data input was valid, complete, and accurate to electronic sources
- Passing data between the related transactions to minimize data entry and improve data consistency
- Automatically recording the accounting transaction upon data input
- Automatically reconciling the payables subsidiary ledger to the general ledger
- Generating exception and analytical reports

As a result of the implementation, management of Insight Media gained access to more

accurate, complete, and timely information to perform internal controls over the evaluation of accounting entries and disclosures for accounts payable and accrued expense balances, purchasing commitments, and expected cash balances.

The following flowchart was created as a result of the above procedures and assisted management in identifying the relevant information.



Key Areas Legend:

- **A** Passing data between the related transactions to minimize data entry and improve consistency
- **B** Checking that data input was valid, complete, and accurate to electronic sources
- **C** Automatically recording the accounting transaction upon data input
- **D** Automatically reconciling the payables subsidiary ledger to the general ledger
- **E** Generating exception and analytical reports

System/Database | Control | Paper Document

Process | EDI Transmission between application/systems

Approach: **Enhancing Information Quality through a Data Governance Program**

- Identifies Information Requirements
- Captures Internal and External Sources of Data
- Processes Relevant Data into Information
- Maintains Quality Throughout Processing
- Considers Costs and Benefits

Senior management establishes a data governance program to support the company's objectives of ensuring reliability of information used in support of internal controls and external financial reporting. Senior management formalizes policies, procedures, and responsibilities for data and information management considering the volume, complexity, and demand for rapid capture and dissemination from multiple sources. The data governance program includes policies and procedures for:

- Assigning roles and responsibilities between a central data management group, business functions, and IT
- Validating sources of information
- Establishing data-quality requirements before accepting sources into the information system
- Accessing rights to underlying data and related information produced through processing
- Protecting data during transmission and storage

Example: **Validating Data and Information**

RightChoice Pharmacy, Inc., a national drugstore chain, obtains significant data underlying transactions recorded in point-of-sale systems located at each retail store. Data underlying credit card transactions is sent immediately to the credit card company and to RightChoice's internal data warehouse. Daily reports are produced from the data warehouse and used to prepare reconciliations of payments due from the credit card companies.

The chief information officer and the credit and collections manager have designed and implemented continuous transaction monitoring software to support their data and information quality efforts. This software helps management to verify accounts receivable balances each day and to avoid time-consuming month-end reconciliations by quickly identifying data anomalies. Targeted data queries allow the software to identify duplicate entries, unusual transactions, missing data, and incomplete data transfers. Additionally, continuous monitoring software enables data analysis used to support control activities to detect potential indicators of fraud.

Approach: **Identifying, Securing, and Retaining Financial Data and Information**

- Identifies Information Requirements
- Captures Internal and External Sources of Data
- Processes Relevant Data into Information
- Maintains Quality Throughout Processing
- Considers Costs and Benefits

Senior IT management establishes policies to define categories of data and assign requirements for securing and retaining the data. These policies support management and employee responsibilities for securing information from unauthorized access or change and for adhering to retention and data destruction requirements. The senior data administrator develops processes and repositories to carry out the data classification policy. Data classification requirements are communicated to personnel responsible for transaction processing through periodic reminders on important internal control

responsibilities. Important to this process is considering the benefits and costs to manage and store information and the relative value of the information to the entity.

Example: **Identifying and Protecting Financial Data and Information**

Bio-Adaptive, Inc., a global life science and chemical manufacturer, has developed standard operating procedures to identify, classify, and secure sensitive information, including financial information, throughout the data and information life cycle (input, processing, output, storage). These procedures include, but are not limited to:

Bio-Adaptive, Inc., a global life science and chemical manufacturer, has developed standard operating procedures to identify, classify, and secure financial data and information across the entity and the stages of information life cycle (input, processing, output, storage). As part of these procedures, personnel:

- Confirm adherence to standard operating procedures
- Identify financial data and information that requires restriction of access and retention in order to meet reporting requirements
- Assign appropriate data security categories to sensitive financial data and information when input into the information system
- Review automated application controls that support security, privacy, and storage of financial data and information based on the data security category input
- Review periodically that sensitive financial data and information have been properly categorized[22]

Example: **Identifying and Classifying Data for Financial Reporting**

Freedom Corp., a financial services firm, has a process to tag financial data during transaction processing based on criteria established in the company's data classification policy. Business and IT personnel who are involved in detailed transaction processing are trained in data entry to support accurate and complete classification, tagging, storage, retention, and disposal.

This process reduces the time required to format, organize, and report data. It also enables the company to tag data through eXtensible Business Reporting Language (XBRL). XBRL enables Freedom Corp. to meet certain external financial reporting requirements and to perform comparative analyses to historical, competitor, and projected financial data.

22 This example is continued in Chapter 6, Monitoring Activities, to illustrate how monitoring activities may assess whether controls to effect principles in information and communication are deployed as intended (see page 147).

Communicates Internally

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

Points of Focus

The following points of focus highlight important characteristics relating to this principle:

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

Approaches and Examples for Applying the Principle

Approach: **Communicating Information Regarding External Financial Reporting Objectives and Internal Control**

Senior management communicates information about the company's financial reporting objectives, financial control requirements, and internal control policies and procedures, and how they support individual responsibilities through a variety of communication channels. The method of communication varies depending on the audience; the nature of the information; time sensitivity, cost, legal, or regulatory requirements; and ability to use technology solutions. Such mechanisms may include:

- Departmental vision and mission objective signposts in high-traffic areas or on the company's website
- Accounting and finance internal meetings or conferences to discuss internal control matters and accounting policy changes
- Periodic employee surveys related to awareness and compliance to internal control policies and procedures
- An intranet site specific to internal control matters, including code of conduct, roles and responsibilities, policies, procedures, and other relevant matters
- Regular organization-wide emails, newsletters, conference calls, webcasts, or meetings about updates on internal control matters
- Senior finance and executive management visits to plants, sales offices, major customers, and other locations

- Communicates Internal Control Information
  - Communicates with The Board of Directors
  - Provides Separate Communication Lines
- Selects Relevant Method of Communication

Example: **Using Communications Programs to Reinforce Internal Control**

AtHome Corp. is a global home-building company. Both the CEO, Janis Wilcox, and the CFO, Terry Tomlinson, use regular broadcast emails and personal visits to various company sites to communicate with finance, accounting, and other personnel who impact internal control over external financial reporting.

Mr. Tomlinson uses these mechanisms to reinforce company expectations for adherence to internal control over external financial reporting, laws, and regulations; the importance of the company's internal audit function; and actions taken in response to internal audit findings and internal control recommendations from its external auditors.

In turn, Ms. Wilcox finds the broadcast emails an effective means of sharing information about the company's business objectives and goals, including a periodic update on progress toward those goals. She also visits the various corporate sites and meets with employees and managers to ascertain how well they understand key business and financial objectives relevant to their sites and to reinforce the messages about internal control from Mr. Tomlinson. Presentation material and supporting information and intranet links are provided to the participants to support these communications.

Example: **Using an Internal Accounting and Finance Conference to Reinforce Policy Changes**

NetComm, Inc., a broadband infrastructure company, holds a semi-annual meeting led by the CFO and controller. The personnel from the finance department attend these meetings to obtain updated information on significant new or changed matters that impact finance activities and financial results. Meeting topics routinely include:

- Key objectives for the next six months
- Reinforcement of the company's policies related to ethics and integrity
- Expectations regarding recent findings from internal or external audits related to financial reporting and control
- Changes to the internal control structure
- Significant recent or anticipated events such as the sale of a business, acquisition of assets, restructuring of operations, or introduction of a new product
- Changes to accounting policy and regulatory rules that would impact how the company processes its financial transactions and produces its financial reports

Approach: **Communicating Internal Control Responsibilities**

- Communicates Internal Control Information
- Communicates with The Board of Directors
- Provides Separate Communication Lines
- Selects Relevant Method of Communication

Documentation on internal controls related to financially significant business processes and systems is stored in a shared repository that is accessible to management and personnel who are responsible for external financial reporting. This repository contains:

- Risk assessment documentation
- Business process documentation, including process flow diagrams and supporting narratives
- Internal controls identified by management based on risk assessments
- List of individual internal controls, including assignment responsibility for performance and review/approval to specified employees and management

The internal audit department reviews the information in the repository as part of its ongoing and separate evaluations. Updates to specific internal controls are communicated to both the control performer and reviewer through email alerts with links to the repository.

Example: **Using Governance, Risk, and Compliance Technology to Manage Internal Controls**

A manufacturer of chemical and pharmaceutical products, Travis Pharma, has implemented a governance, risk, and compliance technology solution. This provides the CFO, Frances VanWyck, with a reporting tool to support her oversight of the system of internal control over external financial reporting. Information communicated through the tool includes:

- External financial reporting objectives
- Related external financial reporting risks
- Internal controls
- Evaluation approaches for each control
- Responsibility for performance and review of each control
- Evaluation results and action plans to address deviations

The reporting tool also provides a personalized dashboard; workflow process (for performance or review, as appropriate); reporting capabilities for more detailed status, issues, and trends; and other information to understand and manage the individual's internal control responsibilities.

Approach: **Developing Guidelines for Communication to the Board of Directors**

The Board of Directors establishes a board charter that defines the guidelines for information to be shared with the board of directors, responsibilities for communication, and the method of communication. The charter specifies key guidelines, which may include:

- Frequency and number of board meetings, including committees of the board
- Objectives of each board or committee meeting (e.g., strategy reviews, annual budgets, and plan reviews)
- Nature and extent of information to be shared for each meeting
- Responsibility for preparing and approving minutes

Example: **Facilitating Communication between Executive Management and the Board of Directors**

Fred Cummins, the general counsel of a printing company, EasySigns, Inc., under the direction of the chair of the board, is responsible for coordinating all meetings of the board of directors and board committees. He has implemented a straightforward system to ensure timely and effective communication.

Mr. Cummins reviews the annual calendar of audit committee meetings and the general agenda for each meeting. He develops specific topics for discussion for each meeting relevant to the company's external financial reporting requirements and confirms the agenda details with the CFO, CAE, and audit committee chair. Based on the detailed agenda, Mr. Cummins gathers relevant information to be included in the audit committee meeting materials that are sent to members one week prior to the meeting. From time to time, he requests that members of management attend meetings to present information in person and allow for active communication. For example, the CIO presents on the company's security and privacy programs and new events that may impact risks.

Communicates Internal Control Information
- Communicates with The Board of Directors

Provides Separate Communication Lines
- Selects Relevant Method of Communication

Mr. Cummins also meets with the chair of the audit committee on a periodic basis to communicate issues or risks related to significant, time-sensitive transactions, or to update the audit committee chair on significant issues, such as investigations of potential fraud.

Approach: **Reviewing Financial and Internal Control Information with the Board of Directors**

Communicates Internal Control Information
- Communicates with The Board of Directors

Provides Separate Communication Lines
Selects Relevant Method of Communication

At designated board meetings the CFO and supporting personnel present financial information, provide an analysis of the results compared with expectations, give updates on forecasts and major changes to original budgets, and communicate other matters of significance to financial reporting.

On a regular basis, the CEO, CFO, and the chief audit executive (CAE) present the draft external financial statements. Material events, changes in significant estimates, or assumptions and significant new disclosure matters since the prior quarter are also presented and discussed. The external auditors attend these meetings to present their point of view on the financial statements.

At each quarterly meeting, the CFO and the CAE present a summary of key changes in internal control, results of evaluations, and actions in response to any deviations identified. Matters of significance are reported in writing. The audit committee holds separate private sessions with management and the external auditors. These sessions provide the audit committee and either management or the auditors with an opportunity to share sensitive information and ask probing questions that facilitate each party's responsibilities related to internal control.

Example: **Preparing Financial and Internal Control Reporting Package for Discussion with the Board**

The senior financial management at a privately held mining company, Precious Metals Corp., has developed a financial and internal control reporting package for the board meeting. The package has been developed from both quantitative and qualitative financial reporting and internal control information. It highlights financial and internal control trends and internal control matters requiring the board's attention, such as significant, non-recurring adjustments and internal control deficiencies by each financial statement line item for each of the last four quarters. Other information in the package includes:

- Dollar impact of adjustments
- Estimated impact of deficiencies after considering compensating controls
- Brief description of severity of issues, business function, and processes impacted
- Management point of contact and action plan
- Changes in accounting policies
- New regulatory requirements
- Significant changes in financial statements and disclosures

The management team sends the package to the board in advance of the meeting to allow board members to review and follow up with management in preparation of the meeting, if necessary.

Approach: **Communicating a Whistle-Blower Program to Company Personnel**

Management and the board establish a whistle-blower program for employees to use a hotline to communicate concerns, instances of perceived misconduct, matters relating to external financial reporting, or other significant matters that may impact internal control. To enhance employee awareness of the program, a number of communication channels are used. These include postings in high-traffic areas in offices and periodic messages from the director of human resources.

The program allows employees who report matters through the hotline to remain anonymous, and all communication is completely confidential. Reported matters are evaluated by an objective party and communicated to the board of directors or, where appropriate, a specified delegate (such as the audit committee or internal audit).

Communicates Internal Control Information

- Communicates with The Board of Directors
- Provides Separate Communication Lines

Selects Relevant Method of Communication

Example: **Employee Ethics Hotline**

General Goods Packaging has established a toll-free hotline for employees to report misconduct. The hotline is described in the employee handbook and on the company intranet. Information is also posted at various high-traffic locations in the company's facilities, such as the cafeteria, coffee room, restrooms, and main entrance.

The hotline is administered by a third party. All matters received on the line are categorized, summarized, and reported to a separate compliance department that reports to internal audit. The director of compliance then reviews and prioritizes all reports.

Those matters of significance or heightened sensitivity are reported immediately to the chair of the audit committee. Others are investigated based on their priority. The members of the executive management team review the results of all investigations and recommend what actions should be taken.

Information about each reported matter, including evidence gathered, actions taken, and conclusions reached, is documented in a separate, confidential section of the hotline system.

Approach: **Communicating through Alternative Reporting Channels**

Management provides an alternative to reporting to a line manager so that employees are confident that they will be heard. Alternative reporting and communications channels may include:

- Mentoring programs to provide employees with a support structure beyond their direct line manager

Communicates Internal Control Information

Communicates with The Board of Directors

- Provides Separate Communication Lines

Selects Relevant Method of Communication

- Town hall meetings where employees are encouraged to ask questions and discuss their concerns
- A staff council comprising employees from various departments and various levels below manager which meets to discuss various issues and relays comments and observations to management

Example: **Establishing a Mentoring Program to Encourage Communicating with Management**

Odette Group, a designer and distributor of sports apparel, has established a successful mentoring program for its employees. Every employee is assigned an individual "coach," who is selected from management of a different department. The employee and coach meet quarterly, or as needed, to discuss topics such as the employee's long-term goals, areas of interest for growth and development, and results of periodic performance reviews. At these meetings, coaches encourage employees to provide feedback on any issues or concerns for which they did not see a clear communication channel.

As an added measure, all staff involved in the financial reporting process is assigned a mentor with financial reporting and internal control experience. This provides an alternative to the employee's line supervisor for discussing and reporting concerns on matters such as compensation, operations, or internal controls.

Approach: **Establishing Cross-Functional and Multidirectional Internal Control Communication Processes and Forums**

- Communicates Internal Control Information

  Communicates with The Board of Directors

- Provides Separate Communication Lines

  Selects Relevant Method of Communication

Management from all departments develop cross-functional and departmental communication processes and forums that enable personnel to communicate internal control matters across the entity. Representatives from each department have defined roles and responsibilities for communicating internal control matters using these processes and forums. The group meets periodically to discuss issues, trends, and upcoming events that impact internal controls. Control matters and issues noted by a shared service center, business unit, or department are communicated to the other departments and business units. Management and personnel in the departments and business units evaluate and respond to the impact of these matters and issues.

Example: **Establishing a Cross-Functional Internal Control Committee**

Sea to Sky Telecommunications has established an internal control council comprising functional and IT business process owners from each business unit, corporate accounting, shared service center, and internal audit. The council meets monthly to define information that should be shared among business units and that may impact company processes. Topics raised at these meetings include:

- Incidents of fraud in one department that may impact other departments
- Changes to systems that have a cross-functional impact on processes and controls

- Changes to regulations that impact how different departments exchange information
- Internal and external audit findings

The representatives on the council review all matters raised to consider how they impact the various departments of Sea to Sky. Council members take turns recording the meeting proceedings, which are reviewed by all council members and then shared with the CFO.

Communicates Externally

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

Points of Focus

The following points of focus highlight important characteristics relating to this principle:

- **Communicates to External Parties**—Processes are in place to communicate relevant and timely information to external parties, including shareholders, partners, owners, regulators, customers, and financial analysts and other external parties.
- **Enables Inbound Communications**—Open communication channels allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others, providing management and the board of directors with relevant information.
- **Communicates with the Board of Directors**—Relevant information resulting from assessments conducted by external parties is communicated to the board of directors.
- **Provides Separate Communication Lines**—Separate communications 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, nature of the communication, and legal, regulatory, and fiduciary requirements and expectations.

Approaches for Applying the Principle

Approach: **Communicating Information to Relevant External Parties**

Management considers all relevant external parties who have an interest in or who would be reasonably expected to obtain information about the company's internal control over external financial reporting. The company's disclosure committee (or similar group responsible for external communications) has established a process to evaluate ongoing company events, policies, activities, and other matters that impact external parties that are important to the company's external financial reporting objectives. The disclosure committee determines the information that should be reported to external parties, as needed. Such information may include:

- Internal controls over transactions and balances that represent significant payables, receivables, or commitments to external stakeholders
- Results of procedures for monitoring compliance with contractual commitments and related loss or damages provisions
- Policies for protecting information received from external parties during normal business transactions
- Customer responsibilities for managing their employees' access to the company's web-based ordering system to prevent unauthorized orders
- Policies related to performing background checks and credit checks, or using collection agencies

- Communicates to External Parties
- Enables Inbound Communications
- Communicates with The Board of Directors
- Provides Separate Communication Lines
- Selects Relevant Method of Communication

Example: **Communicating Internal Control Information to a Federal Agency**

A federal agency is responsible for managing and overseeing the distribution of approved funds to not-for-profit organizations that provide community outreach programs for underprivileged children. In connection with its oversight responsibilities, the federal agency requests information from each community organization about its program's controls over the allocation and use of funds received.

Management of each community organization summarizes their control activities over the allocation and use of funds and provides a statement that control activities were designed, implemented, and operating for the quarter. Any changes to or deterioration in the controls, such as changes in ability to segregate duties due to loss of personnel, are communicated along with management's actions to mitigate risks. This summary is provided quarterly to the federal agency.

Example: **Establishing Periodic Communications with Contractors and Outsourced Service Providers**

ConFab Group, a large, privately held telecommunications equipment provider, outsources all its manufacturing activities to third parties, which are located around the world. Under the contractual arrangements, ConFab is responsible for damage or loss of inventory from the receipt of raw materials at the third-party contract manufacturer until the completed products are delivered to the freight forwarder for shipment. This means management retains significant risk to inventory that is not within its physical control.

ConFab's management team has specific policies and procedures for the purchasing, manufacture, and preparation of shipments to mitigate its economic exposure and that support its estimates for inventory reserves. Management communicates these policies to the manufacturers, along with specific contract clauses that require adherence to the policies and the right to audit by the company.

To ensure that policies and procedures are carried out as intended, ConFab has implemented several methods of communicating with the contract manufacturers:

- A website is built specifically for communications between the company and the contract manufacturers.
- A link is provided on the company's website to policies and procedures, which contractors are required to acknowledge they have read and understood, and that they will adhere to it.
- A variety of periodic reports from the contract manufacturers are provided, which are used in company control activities to ensure that inventory balances and related estimates are properly reported.
- Periodic on-site audits at contract manufacturers are peformed to validate the inventory quantities on hand, stage of production, and quality. The audits include random interviews of personnel to confirm their understanding and adherence to policies and procedures and inspection of inventory transactions, documents, and reports.

ConFab also performs annual reviews of the contract manufacturers' controls that support the completeness and accuracy of reports provided throughout the year.

Approach: **Obtaining Information from Outside Sources**

Communicates to External Parties
• Enables Inbound Communications
Communicates with The Board of Directors
Provides Separate Communication Lines
Selects Relevant Method of Communication

Management and other personnel stay abreast of new matters relevant to their area of responsibility in order to identify and respond to changes that may impact, directly or indirectly, external financial reporting objectives or the related internal control. Management of each business unit or functional group identifies relevant means to receive information from outside the company, and assigns responsibility to themselves and other personnel to be responsible for obtaining, reviewing, and sharing relevant information within the company, as appropriate. Sources of information may include:

- Publications that provide updates to financial accounting, reporting, and disclosure standards or regulations
- Technical journals that analyze the impact of financial accounting and reporting matters
- Competitor or peer regulatory filings
- Information gathered at industry or trade association meetings

- Industry, market, economic, or competitor data relevant to key metrics or accounting estimates
- Alerts from outside counsel on regulatory or legal changes
- Periodic meetings with external auditors and advisors to understand new accounting and disclosure requirements
- Meetings with outside advisors or subject matter specialists with the expertise to assess complex accounting and disclosures for major transactions or events
- Standard-setter and regulator projects and publications
- Postings on organization-sponsored or supported social media websites or communication tools

Example: **Communications from Regulatory Bodies**

As a result of a regulator's examination, Norgaard-Kellogg Financial, a registered investment advisor, was informed that the firm was not in compliance with rules requiring documentation of certain compliance policies and procedures for trading activities and the related accounting and disclosure requirements. Eileen Nachbar, the company CFO, met with outside counsel and external auditors to review the matters and obtain their views. She also engaged other external advisors with expertise on risks and best practice procedures related to trading activities.

After these discussions, Ms. Nachbar met with the senior management of Norgaard-Kellogg responsible for trading activities to discuss the regulator's findings and her own evaluation of the issue and recommendations for enhancements. The information was shared with the disclosure committee, a group responsible for assessing the requirements for disclosures in external filings. After approval of the proposed actions by the disclosure committee, Ms. Nachbar developed an action plan for updating internal control policies, procedures, and related documentation to address the compliance requirements.

Example: **Obtaining Information from External Sources to Assist with Accounting Estimates**

Nevio Group regularly sells its products in highly unstable economic environments where currency values fluctuate significantly. These fluctuations significantly affect the accounting treatment of transactions and balances recorded in the financial statements.

Clint Bell, the assistant treasurer, is responsible for obtaining and analyzing information from an outside advisory firm related to the past, present, and future expectations of currency fluctuations. One of his sources is a subscription service that provides reporting on currency values, changes in values, and trends over periods of time. It also provides alerts if currency fluctuations exceed certain thresholds.

Mr. Bell sets up the relevant currencies, time periods, and alerts appropriate for Nevio Group. The treasurer reviews the settings and approves changes, if needed, each quarter. On a monthly basis, or more frequently based on alerts received, Mr. Bell evaluates the currency rates used for financial accounting associated with significant estimates impacted by currency values.

Based on the information gathered and corroborated from various external sources, he updates his analysis estimates. The analysis is given to the treasurer, director of financial reporting, and controller to help them ensure that the basis for their estimates and communications in external reports is current and appropriate.

Approach: Surveying External Parties

Communicates to External Parties

- Enables Inbound Communications

Communicates with The Board of Directors

- Provides Separate Communication Lines

Selects Relevant Method of Communication

Management surveys customers, vendors, and others on their perception of the integrity and ethical values of company personnel. This survey process is controlled by company personnel independent of the main customer/vendor contacts. These surveys not only provide a sounding board for the company's customers, but also enable management to gain important information about the commitments made to customers and ensure that such commitments are consistent with the understanding of formal arrangements between parties.

Management carries out surveys of external parties in a variety of ways, which may include:

- Sending to all customers periodic surveys with standard questions regarding the company and its products or services
- Providing a feedback mechanism on the company's website or through a feedback box on documents that are sent regularly to external parties
- Periodically meeting with external parties, in person or by video or teleconference

Example: **Conducting Discussions with Customers**

Fitness Four, a manufacturer of strength and cardiovascular fitness equipment, has developed a policy requiring a member of management to contact each customer at least annually. The management team member must not be the customer's primary contact or in any senior line of reporting of the customer's primary contact at the company.

During these discussions with customers, the manager is expected to address a number of areas relevant to the customer-company relationship that impact external financial reporting, including:

- Customers' adherence to acceptable use provisions based on licensing rights that may impact royalty costs
- Confirmation of continued use of products or services that may impact the estimated life of assets or term of contracts used for accounting judgments
- Issues, concerns, or return activity of company products that may indicate that recorded sales transactions were not valid
- Feedback on company individuals that the customer interacts with during the sales, delivery, support, customer service, or billing process
- Any regulatory, compliance, or internal customer policy requirements that should be considered in the manufacture of products or provision of services

- Expectations of the customer for additional products, services, or support that may indicate commitments made outside of the contracts or other written arrangements

The information gathered through these conversations is shared with finance and other relevant company personnel. Any issues that indicate a potential financial reporting issue, such as incomplete delivery of products or services, or billing and payment, are further investigated. Where changes in the accounting for transactions are needed, additional reviews are performed to ensure that the issues are fully resolved. Also, an evaluation of internal controls for deficiencies is conducted to prevent or detect issues from recurring.

Approach: **Communicating the Whistle-Blower Program to Outside Parties**

- Communicates to External Parties
- Enables Inbound Communications

  Communicates with The Board of Directors
- Provides Separate Communication Lines

  Selects Relevant Method of Communication

Management provides a whistle-blower phone number or email address to customers, suppliers, outsourcing companies, and other external parties to facilitate feedback on potential improprieties or improper or unreliable financial reporting. The contact information is disseminated through various means, such as the company's website and on invoices sent to customers.

Example: **Facilitating Communication with External Parties**

Shoreup Nutrients is a manufacturer and retailer of branded and private label vitamins and nutritional supplements. It provides a section on its website for anyone who wants to respond with questions, concerns, complaints, or other information.

The internal audit department of Shoreup Nutrients is responsible for maintaining a process to ensure that all reported matters are collected, documented, evaluated, and addressed appropriately. On a weekly basis, internal audit monitors the website and summarizes any new information collected by using a collaboration software tool accessible only to the audit department.

The director of internal audit, Naseema Bahair, evaluates each matter and develops an action plan, which includes:

- Conducting interviews of company personnel
- Obtaining and reviewing relevant documentation
- Contacting the reporting party for additional information, if necessary

Upon review of complaints received through whistle-blower hotlines, a decision is made by the CFO or the audit committee chair about the information that will be shared to the reporting party.

Communicates to External Parties

- Enables Inbound Communications
- Communicates with The Board of Directors

Provides Separate Communication Lines

Selects Relevant Method of Communication

Approach: **Reviewing External Audit Communications**

Following the external auditor's review of financial information and independent evaluation of internal control effectiveness, management receives a written summary of significant matters identified during the course of the work. The board of directors discusses these at a subsequent meeting, where external audit personnel discuss their findings and management discusses proposed resolutions.

Example: **Managing and Assessing External Audit Communications**

The management at Hessen's Assure, a healthcare insurance company, has established a process with the external audit firm to coordinate the periodic assessments of internal controls and discuss and respond to matters identified during the course of the external audit. The management team meets monthly with the external auditor to discuss internal control testing plans, status, and issues.

Internal control issues or recommendations for improvement that are identified by the external audit firm are assigned to an employee in the impacted business process area, and that person develops and presents a recommended response at the monthly meeting, or more frequently if needed. The management team evaluates each response, such as modifying internal control activities; reinforcing awareness; updating policy, procedure, or control documentation; or performing additional evaluations, and assigns responsibility for carrying out the response.

Results of the management meeting are communicated to the external audit firm. As well, a summary of significant issues and observations are presented at the audit committee meeting at set intervals during the year or as necessary.

6. Monitoring Activities

Chapter Summary

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

Principles relating to the Monitoring Activities Component

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

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

Principles	Approaches
16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	• Periodically Reviewing the Mix of Monitoring Activities • Establishing a Baseline • Identifying and Using Metrics • Designing and Implementing a Dashboard • Using Technology to Support Monitoring Activities • Conducting Separate Evaluations • Using Internal Audit to Conduct Separate Evaluations • Understanding Controls at an Outsourced Service Provider
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.	• Assessing and Reporting Deficiencies • Monitoring Corrective Action • Developing Guidelines for Reporting Deficiencies

Conducts Ongoing and/or Separate Evaluations

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

Points of Focus

The following points of focus highlight important characteristics relating to this principle:

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

- Considers a Mix of Ongoing and Separate Evaluations
- Considers Rate of Change

Establishes Baseline Understanding

Uses Knowledgeable Personnel

Integrates with Business Processes

- Adjusts Scope and Frequency

Objectively Evaluates

Approaches and Examples for Applying the Principle

Approach: **Periodically Reviewing the Mix of Monitoring Activities**

Senior management meets periodically to review the allocation of effort between ongoing evaluations and separate evaluations used to conduct monitoring activities. The mix of planned monitoring activities over internal control of external financial reporting may depend on senior management's assessment of:

- The entity's regulatory requirements and financial reporting objectives
- How quickly the entity's industry and/or regulatory environment is changing or anticipated to change
- The results of historical evaluations of control effectiveness
- The extent of ongoing monitoring within the associated processes
- Changes that have occurred in the current year that impact other components of internal control

Senior management may also increase the frequency of separate evaluations from the initial plan in processes where:

- Existing monitoring activities raise potential deficiencies in the system of internal control
- Key performance indicators, which correlate to surfacing potential deficiencies in internal control, have exceeded a prescribed threshold

Example: **Changes in Business Operations**

Hunter Manufacturing has thirteen different plant locations, six of which are considered significant. The management team of Hunter Manufacturing has been monitoring the internal control in the seven smaller, less significant plants, primarily through ongoing evaluations. However, management has now determined that some separate evaluations have become necessary. This decision has been made due to the increase in risk factors at these plants, including frequent errors in monthly and quarterly reconciliation activities and turnover among plant-level controllers and supervisory personnel. Accordingly, management now has both ongoing and separate evaluations in place as they have implemented random plant audits to periodically evaluate controls.

Example: **Changing the Internal Audit Plan**

Viliam Financial Services is a publicly held global company. Recently the industry has experienced a significant rate of change because of increasing regulatory focus and complexity of the company's financial products. In response to these changes, Viliam's management and board of directors have reprioritized the activities conducted by its internal audit department, including:

- More active oversight of Viliam's recently enhanced risk management and governance processes
- An iterative risk assessment process that performs a risk review annually and more often if the business changes

- Reviews of financial and operational data to identify risks and adverse trends, and to respond to them accordingly by conducting targeted audits

Approach: **Establishing a Baseline**

Senior management develops a baseline understanding of the design and current state of the entity's system of internal control by:

- Determining the starting point of the system
- Reviewing if controls within each of the five components of internal control are operating as intended to achieve an entity's objectives

Management then leverages the established baseline to:

- Identify necessary changes in design and conduct of internal controls that result from monitoring activities
- Evaluate changes in people, processes, and technology that may impact the design and implementation of controls
- Establish a new baseline that incorporates any changes that impact the previous baseline

Senior management may use the baseline information to establish which ongoing and separate evaluations are most appropriate.

Example: **Establishing a Baseline**

The senior management of Judd Co., a beverage manufacturer and distributor, focuses the organization's monitoring efforts by risk priority. In areas of high risk the entity conducts and documents a thorough review of the design and operation of controls to establish a baseline. The documentation includes a written description, flowchart, and walkthrough narrative of how each control within the high-risk area operates. Past and current control performance must also be documented with any anomalies or significant variations noted and evaluated. With risks prioritized and the baseline established, management identifies monitoring activities that can evaluate changes to the system of internal control in a reasonable period of time. The baseline aids Judd Co. in selecting more efficient monitoring activities, such as self-assessments coupled with supervisory review. Then, at intervals appropriate to the level of risk, internal audit performs periodic separate evaluations to reconfirm the system of internal control against the baseline and the effectiveness of the ongoing monitoring procedures.

Considers a Mix of Ongoing and Separate Evaluations
Considers Rate of Change
• Establishes Baseline Understanding
Uses Knowledgeable Personnel
Integrates with Business Processes
Adjusts Scope and Frequency
Objectively Evaluates

Considers a Mix of Ongoing and Separate Evaluations
Considers Rate of Change
• Establishes Baseline Understanding
Uses Knowledgeable Personnel
• Integrates with Business Processes
Adjusts Scope and Frequency
Objectively Evaluates

Approach: **Identifying and Using Metrics**[23]

Management identifies metrics that correlate to the completeness and accuracy of financial transactions to provide ongoing evaluations of established control activities. When identifying metrics, management considers the processes and sub-processes that should be monitored, and develops the appropriate measure and frequency for the evaluation.

The metrics may use the following information:

- Historical performance data, which may be useful for comparisons to current performance data
- Expected performance targets, which may be used to benchmark current performance against expected performance

Some metrics have clearly defined allowable tolerances that have been calculated for current performance data, which may be used to highlight anomalies. Other metrics have less defined thresholds and are reviewed by knowledgeable employees for reasonableness and unusual items.

Example: **Using Metrics to Monitor Payroll**

Approximately 90% of Mynarski Manufacturing employees are located at company plant sites. To monitor whether the payroll processing control activities are working, Henrik Saunders, the corporate payroll manager, reviews the plant payroll metrics. Payroll metrics include:

- Current head count compared with expected and historical head count for the month, quarter, and year
- Current payroll compared with expected and historical payroll for the month, quarter, and year
- Current overtime in hours and dollars compared with expected and historical overtime in hours and dollars for the month, quarter, and year

In his review, Mr. Saunders looks for any unusual fluctuations, such as increases and decreases in the number of employees and excessive overtime. His review is done in the context of current plant productivity and target thresholds based on historical data and planned productivity, which varies by season. If Mr. Saunders identifies any fluctuations, he investigates the underlying reasons and adjusts the process or control activities as needed.

23 Metrics, often operational in nature, may use information that indirectly signals a failure or anomaly, but there may be other information available more directly linked to changes or failures. The value of metrics should be considered when an entity evaluates what mix of ongoing and separate evaluations is appropriate for that entity.

Example: **Using Built-In Operating Measures and Key Control Indicators**

Tony Rosco is the controller of Still Craft Foods. He uses operating measures and key performance indicators (KPIs) for major accounting and financial processes, including accounts receivable, payroll, accounts payable, and financial statement preparation. Accounts payable KPIs, for example, focus on the accuracy, timeliness, completeness, and compliance of documents received for vouching and checks prepared, with performance tracked to established targets.

Mr. Rosco leverages his knowledge of changes in the business when developing his expectations on how performance is likely to be consistent with, or vary from, established targets. In the case of accounts payable KPIs, those variances from the established targets could result from known factors, such as significant new vendors, changes in payment terms, and cash flow goals. Where results do not meet expectations, Mr. Rosco evaluates them for potential underlying issues in established control activities. Additionally he uses the KPIs to identify trends that could indicate some fraudulent activity (e.g., he sees a concentration of payments to a vendor that is new or for which he would not expect that volume).

He shares his findings with the management team, which uses the information in performance appraisals and related development programs.

Approach: **Designing and Implementing a Dashboard**[24]

As part of its ongoing evaluations, management develops and implements dashboards for reviewers to use in the ordinary course of business. Reviewers are usually supervisors of those employees with first-level knowledge and who are accountable for processes, activities, and their controls. Dashboards may include:

- Detailed and/or summarized information about control performance
- Metrics being measured and/or information being highlighted for evaluation and investigative follow-up
- Visual depictions of the status of control operation
- Details of status including frequency of assessment and last assessment
- Known current deficiencies and their remediation status
- Key personnel and contact details for those responsible for processes and sub-processes

Considers a Mix of Ongoing and Separate Evaluations
Considers Rate of Change
Establishes Baseline Understanding
- Uses Knowledgeable Personnel
- Integrates with Business Processes
Adjusts Scope and Frequency
Objectively Evaluates

24 A dashboard, a management tool or report that presents in a summarized manner data on the relevant business performance areas, is often operational in nature and may use information that indirectly signals a failure or anomaly, but there may be other information available more directly linked to changes or failures. The value of metrics should be considered when an entity evaluates what mix of ongoing and separate evaluations is appropriate for that entity.

Example: **Using Dashboards to Relate Operating Information**

Langdale Manufacturing, a manufacturer of industrial machinery parts, uses a set of operating dashboards by business process, with each dashboard containing a series of tasks assigned to the appropriate managers for action. The dashboard for the production inventory process, for example, includes costs associated with tooling: where the warehouse manager checks the usage of tools during production noting how often they are needed, who requested them, and where they are purchased from.

Management then considers this information when reviewing tooling costs included in inventory. In the monthly management meetings, these dashboards are reviewed. Each of the managers responsible for specific tasks discusses recent progress and expected changes over the coming month. To the extent that an increase in tool usage was noted, management would expect that costs related to tooling would be up for the period.

Approach: **Using Technology to Support Monitoring Activities**[25]

Considers a Mix of Ongoing and Separate Evaluations
Considers Rate of Change
Establishes Baseline Understanding
Uses Knowledgeable Personnel
• Integrates with Business Processes
Adjusts Scope and Frequency
Objectively Evaluates

Management uses technology to support the monitoring of the system of internal controls in the ordinary course of business through automated monitoring applications. Management uses the automated monitoring application to efficiently and continuously review large volumes of data at a low cost with a high standard of objectivity (once programmed and tested). Automated monitoring activities may include:

- Checking transactions against predefined thresholds for anomalies
- Monitoring transactions for trends or patterns
- Assessing automated performance indicators, metrics, and measures that may lead to improvements in process and business

Example: **Using Continuous Monitoring**

Gentoo Financial Services employs a continuous monitoring tool to perform a simple regression analysis of nonperforming loans by branch and by loan officers as one form of monitoring control over loan origination. The output from the tool allows Gentoo to look for outliers across multiple dimensions (e.g., policy, industry standards, and statistical standard deviations) and provides input for Gentoo's allowance for loan losses. Further, the report can be repopulated in either real-time or batch mode. This analysis helps Gentoo identify loan officers and/or branches that may not be following loan origination policies.

Example: **Using Technology to Identify Trends**

Penguin Ice, a manufacturer of ice cream, uses an automated computer application as part of its ongoing monitoring activities. One of the application's activities identifies any trends in the processing of journal entries of personnel who consistently approve entries just below their authorization limit. Management then considers this information in

25 Note that many automated activities used to prevent or detect unintended events or results would be considered control activities.

monthly meetings to determine if any fraud is occurring or if journal entry control activities for authorization limits need to be changed.

Approach: **Conducting Separate Evaluations**

- Considers a Mix of Ongoing and Separate Evaluations
  - Considers Rate of Change
  - Establishes Baseline Understanding
- Uses Knowledgeable Personnel
  - Integrates with Business Processes
  - Adjusts Scope and Frequency
- Objectively Evaluates

Management may conduct separate evaluations of internal controls over external financial reporting by:

- Conducting ad hoc supervisory management visits and reviews
- Conducting cross-operating unit reviews using management from similar operating units within the company
- Comparing components of internal control with another similar entity by benchmarking or using a peer evaluation
- Developing a self-assessment questionnaire for a business process for use by personnel responsible for the controls within a particular business unit or function
- Hiring an independent third party to perform specific evaluation

Example: **Investigating and Reporting Whistle-Blower Allegations**[26]

Annually, the board of Generation Now engages an independent third party to evaluate the effectiveness of its whistle-blower program. The purpose of the evaluation is to ascertain that (1) the general counsel has reviewed the logs of all calls received and reported all calls in the quarterly progress reports to the board; (2) the internal auditor (or other independent individual) carried out the investigations into allegations, as necessary, and made recommendations to address any shortcomings in the whistle-blower program; and, (3) all parties complied with the company's policies and procedures in resolving all whistle-blower calls on a timely basis.

Example: **Identifying and Protecting Sensitive Financial Data and Information**[27]

Annually, Bio-Adaptive's chief data officer reviews a system generated report that identifies employees who have access to sensitive financial data and information. For these employees, the chief data officer evaluates the suitability of assigned restricted access and their adherence to the standard operating policies and procedures. Based on the assessment, the chief data officer recommends modifications to existing restricted access, standard operating policies and procedures, and control activities relating to identifying and protecting sensitive financial data and information.

Example: **Conducting Senior Financial Officer Visits**

Gregson Grenville is a publicly held consumer products company with multiple

26 This example is a continuation of the example in Chapter 2, Control Environment (see page 30).

27 This example is a continuation of the example in Chapter 5, Information and Communication (see page 123).

manufacturing facilities throughout the world. Every year, the company's senior financial officers for each division visit each subsidiary's headquarters, manufacturing site, and/or sales office to gain an understanding of significant business processes at those locations. During these visits, the senior financial officer discusses procedures and controls for all relevant processes impacting financial reporting with those performing the control activities and their supervisors. In addition, a mini-audit of select control activities is conducted, the findings are documented, and the local team develops management action plans for all pertinent recommendations. In addition, findings are shared broadly throughout the organization to facilitate control enhancements at other locations, and areas of concern impact the focus of future senior officer visits at this and other locations.

Example: **Using Self-Assessments**

Jaron and Associates provides Internet-based securities brokerage and financial services. Recently the company instituted a formal internal control assessment program (ICAP). Under this program, managers of each business unit perform a quarterly control self-assessment and certify the effectiveness of certain controls for which they are responsible.

The senior management of Jaron recognizes that self-assessment, while not completely objective, is an effective first line of defense against internal control failure. Internal audit helps compensate for the lack of objectivity in the control self-assessments by performing periodic audits and comparing the results to the self-assessments.

ICAP allows management to concentrate its ongoing evaluation efforts on several issues:

- Areas of higher risk
- Areas where ICAP has identified potential problems
- Areas where separate evaluations have identified control deficiencies that were not reported through the self-assessments

Now Jaron and Associates is better able to focus its separate evaluation efforts on a prioritized risk basis and modify ongoing evaluations where necessary.

Approach: **Using Internal Audit to Conduct Separate Evaluations**

- Considers a Mix of Ongoing and Separate Evaluations
  - Considers Rate of Change
  - Establishes Baseline Understanding
- Uses Knowledgeable Personnel
  - Integrates with Business Processes
  - Adjusts Scope and Frequency
- Objectively Evaluates

Management uses an appropriately staffed and adequately trained internal audit function to provide an objective perspective on key elements of the internal control over external financial reporting. Internal audit reports are distributed to senior management, the board of directors, and others who are positioned to act on the report's recommendations. Internal audit's separate evaluations may be influenced by:

- The entity's regulatory environment and management's methodology and plans for achieving compliance with its financial reporting objective
- An understanding, independent of management, of how the internal control system addresses meaningful risks

- Approval for the planned separate evaluation activities by the board of directors or one of its committees

Example: **Identifying and Analyzing Risk of Material Omission and Misstatement due to Fraud**[28]

Maxwell's internal audit considers management's assessments of the likelihood of the risks of material omission and misstatement due to fraud, its planned responses, and the control activities to mitigate these risks when planning its audit projects. Internal audit selects and develops its monitoring activities including the scope, nature, and timing of its evaluations based on its views of the assessed fraud risks and management's planned responses. Internal audit reports these identified fraud risks, along with management's responses and its planned approach, to the chief audit executive and audit committee. Internal audit also discusses the results of its fraud procedures with the external auditor. As part of its approach, internal audit compares any noted fraud incidents to business unit management's fraud risk assessment to identify and evaluate any shortcomings within management's risk assessment process.

Example: **Conducting Separate Evaluations**

Lee-Basker Parts designs, manufacturers, and distributes precision components and assemblies for aerospace applications. From time to time the board directs the company's internal audit department to perform separate evaluations of specified high-risk business processes that impact the entity's financial statements. The scope and frequency of these evaluations depend primarily on the significance of the related risks and importance of the controls in reducing risks to an acceptable level.

Subsequent to management's input, it is up to the chief audit executive, Maria Geide, to determine whether the internal audit department adequately understands the process, the overall internal control structure, and the objectives of the review.

Once the review is complete, Ms. Geide submits a report on the process controls to senior management and the board covering the scope of the work (including identification of the controls evaluated), a description of the major risks and the appropriateness of the controls, a list of identified deficiencies, and management's response and proposed remediation.

Approach: **Understanding Controls at an Outsourced Service Provider**[29]

Management obtains and reviews periodic information from outsourced service providers to detect any changes in activities that impact the entity's system of internal control over external financial reporting. Information obtained may include:

- The outsourced service provider's applicable control objectives

Considers a Mix of Ongoing and Separate Evaluations
Considers Rate of Change
Establishes Baseline Understanding
Uses Knowledgeable Personnel
Integrates with Business Processes
- Adjusts Scope and Frequency
- Objectively Evaluates

28 This example is a continuation of the example in Chapter 3, Risk Assessment (see page 73).

29 The review of controls at the outsourced service provider is covered in Chapter 4, Control Activities.

- Details about which of the outsourced service provider's internal control have been examined and included in any report
- The details and results from any independent audit testing performed
- Special considerations for the outsourced service provider that impacts the report

To determine what impact any identified changes may have on the entity's system of internal control over external financial reporting, the following may also be assessed:

- Whether management appropriately considered known changes in business processes and their impact on internal control, and whether they were communicated to the outsourced service provider, since such changes could impact the entity's control objectives and design
- Whether exceptions were noted that may trigger further review by senior management
- Whether management is satisfied with the independence and objectivity of the report

Based on management's review and findings, it may be necessary to reassess the separate evaluation activities over the outsourced service provider.

Example: **Reviewing the Service Auditor's Report for Changes in Controls**

Finlayson Home Works supplies materials used in residential construction. This public entity has outsourced its payroll activities for a number of years to a reputable payroll services provider. The chief audit executive, Rolf Brunner, obtains an annual service auditor's report detailing the internal controls at the service provider. Mr. Brunner then compares the current report to past reports to determine whether there have been any changes in relevant controls that could impact the judgments made on planned monitoring activities over the payroll process. The current report indicates some key changes in the payroll service provider's software and several negative test results in priority risk areas. As a result, Mr. Brunner has the internal audit department of Finlayson Home Works perform a reconciliation of the payroll service provider's processing results to evaluate if additional separate evaluations of the payroll service provider may be necessary.

Evaluates and Communicates Deficiencies

Principle 17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.[30]

Points of Focus

The following points of focus highlight important characteristics relating to this principle:

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

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

Approaches and Examples for Applying the Principle

- Assesses Results
- Communicates Dificiencies

Monitors Corrective Actions

Approach: **Assessing and Reporting Deficiencies**

Management develops policies and practices to periodically assess and communicate deficiencies that result from the entity's monitoring activities and other sources. Management establishes a practice where all deficiencies in internal control over external financial reporting, regardless of materiality, are reported to the responsible manager and at least one level of management above, both of whom are positioned to take or oversee corrective action. Management also classifies deficiencies for the further reporting to senior management or the board based on criteria established by standard setters or regulators.[31] The criteria could include the following:

- Nature of the deficiency
- Source of the deficiency
- Known magnitude of a misstatement caused by the deficiency to the entity's financial statements
- The likelihood and potential magnitude of a misstatement caused by the deficiency to the entity's financial statements
- An aggregation of deficiencies affecting similar areas that could indicate a more serious deficiency

Example: **Identifying Sources of Deficiencies**

The senior management of Adelie Telecom receives a quarterly report of deficiencies prepared by its internal audit department. On the third-quarter report this year, deficiencies were reported from several sources, including the following:

- *External Source*—Customer complaints about overbilling were brought to management's attention and investigated. The subsequent investigation exposed that the billing system was using the wrong tariff rate, which had been incorrectly coded in the system. The problem was traced to an input error that was neither prevented nor detected by control activities.
- *Separate Evaluations*—Management directed internal audit to conduct a special evaluation of the sources and quality of information used for Adelie Telecom's payroll reconciliation. The evaluation identified that some of the information used was not appropriate. Specifically, an outdated report with inaccurate information was being used for the reconciliation. Consequently, the payroll reconciliation control activity was updated to use the correct report.
- *Ongoing Evaluations*—Adelie Telecom allows a 10% variance in paying installation contractors, and so management developed an automated monitoring control to review the trends in variance activity approvals by payables clerks. One such report identified that Arnie Chinstrap, a payables clerk, was routinely approving

31 For example, in the United States, the SEC issued "Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934." Section B.1. covers the evaluation of control deficiencies that provides management with guidance on the assessment and reporting of deficiencies.

variances of 10% for a particular vendor, Bosque & Sons Installers. An investigation confirmed that Mr. Chinstrap had an arrangement with Bosque & Sons for a financial kickback and that Adelie Telecom was overpaying the contractor. To address the deficiency in internal control, management implemented a supervisory review for all payments within the 10% variance.

Example: **Reporting Protocols for Identified Deficiencies**

The management of Skea and Associates, an international insurance services organization, classifies financial reporting control deficiencies identified from its monitoring activities as deficiencies, significant deficiencies, or material weaknesses. The communication structure for reporting deficiencies is based on their potential impact on the organization.

For each level of deficiency,[32] the company's internal reporting structure calls for certain reporting procedures:

- Deficiencies are reported in detail to the manager responsible for the control.
- Significant deficiencies are reported in detail to the manager responsible for the control and to the senior management team, and on a quarterly basis, in summary, to the audit committee.
- Material weaknesses are reported in detail to the manager responsible for the control and the senior management team, and on a quarterly basis to the audit committee.

Approach: **Monitoring Corrective Action**

Management establishes a practice to review the status of corrective actions taken to verify that reported deficiencies are remediated in a timely manner. The corrective action practice may include:

- Regularly scheduled meetings to review the status of corrective actions
- An established electronic or hard-copy report in which corrective actions are summarized and collated
- Delegated oversight to a responsible party, such as an internal audit function

Assesses Results
Communicates Dificiencies
• Monitors Corrective Actions

Example: **Establishing Reporting Protocols for Identified Deficiencies**

The senior management of Lwiski Manufacturing tracks all control deficiencies identified during monitoring activities and assesses their impact on the organization. These control deficiencies are reported to the management team responsible for the relevant business unit. If necessary, the management team works with internal audit to develop the remediation plan, and internal audit provides oversight to verify deficiencies are remediated in a timely manner.

32 For purposes of this example the deficiency classifications used are those related to external financial reporting in the US as promulgated by the SEC.

Specifically, the plan calls for one individual within the business unit to be assigned responsibility for remediating specific control deficiencies. A time frame for remediation is assigned to each control deficiency, based on its ranking. Working together, management and internal audit verify that deficiencies are remediated within the specified time frame.

Example: **Follow-Up Reporting on Internal Audit Issues**

Mr. James, the chief audit executive of Puna Incorporated, has established a database that tracks management action plans related to issues coming from internal audit reports. Mr. James receives timely updates on the status of actions from business process owners, and also periodically reports to the audit committee summaries of the status of action plans. The reporting includes the percent of action plans implemented on time by business unit.

When sufficient action has not been able to be taken by the business on important internal audit issues by the original reported implementation date, the process owner for the area is invited to attend the audit committee and explain the issues associated with implementation of appropriate actions.

Assesses Results
• Communicates Dificiencies
Monitors Corrective Actions

Approach: **Developing Guidelines for Reporting Deficiencies**

The board of directors develops a shared expectation with senior management on the types of control deficiencies that get reported to the board. The board of directors understands the facts and circumstances regarding internal control deficiencies that impact external financial reporting and provides oversight on management's conclusions and remediation plans.

Example: **Reporting Deficiencies to the Board**

Klemmens and Waters provide air transportation services. The management of the company periodically develops a report of significant deficiencies and material weaknesses, a summary of minor deficiencies, and a summary of past deficiencies. The purpose is to track whether deficiencies are being remediated in a timely manner. The reports are presented to the board for review.

Management has also developed with the audit committee a shared expectation, which states that regardless of the previous categorization, management will report all deficiencies resulting from:

- Illegal or otherwise improper acts
- A significant loss of assets
- Intentional errors and omissions in the conduct of external financial reporting

The audit committee is briefed on the cause of the reported deficiencies and provides oversight of management's assessment of the deficiencies and the actions and status of remediation plans.

Appendices

A: Examples by Topic

Expectations for Governance Oversight

Assessing and Disclosing Director Qualifications *28*

Assessing the Potential of Management Override *30*

Changing the Board Composition of a Closely Held Company *28*

Facilitating Communication between
Executive Management and the Board of Directors *127*

Maintaining Oversight *72*

Reviewing and Documenting Key Activities of the Audit Committee *23*

Reviewing Financial Statement Estimates *29*

Reviewing Governmental Agency Financial Results and Underlying Internal Control *24*

Globalization of Markets and Operations

Automating Balance Sheet Reconciliations *90*

Changes in Business Operations *142*

Conducting Senior Financial Officer Visits *147*

Reorganizing to Support Control Structure *32*

Changes and Greater Complixity in the Business

Aligning Roles and Responsibilities with Objectives *34*

Establishing Periodic Communications
with Contractors and Outsourced Service Providers *133*

Evaluating Business Activities to Identify Information Requirements *115*

Implementing or Assessing Control Activities
when a Report on Controls at a Service Organization is Not Available *87*

Maintaining Control while Engaging Outside Service Providers *34*

Obtaining a Report on Controls
at a Service Organization from a Cloud-Based Service Provider *96*

Obtaining a Report on Controls
at a Service Organization from a Service Payroll Provider *86*

Obtaining Information from
External Sources to Assist with Accounting Estimates *135*

Reorganizing to Support Control Structure *32*

Responding to Significant Change from an Acquisition *77*

Retaining External Tax Assistance *39*

Reviewing the Service Auditor's Report for Changes in Controls *150*

Demands and Complexities of Laws, Rules, Regulations, and Standards

Analyzing Risks from External Factors *68*

Assessing the Suitability of Specified Objectives *54*

Controlling Significant Accounting Estimates *89*

Establishing Policies and Procedures *104*

Establishing Responsibilities for Reviewing Financial Statements *105*

Implementing Complex Accounting Standards *39*

Obtaining Information from External Sources to Assist with Accounting Estimates *135*

Reviewing and Updating Statutory Reporting Requirements *56*

Reviewing and Updating Understanding of Applicable Standards *56*

Using Templates to Document Policies *103*

Expectations for Competencies and Accountabilities

Ad Hoc Assessing of Control Activities *109*

Aligning Competencies with Key Financial Reporting Positions *41*

Assessing and Disclosing Director Qualifications *28*

Assessing the Adequacy of Staffing Levels for Financial Reporting *41*

Audit Committee Review of Managers' Roles *40*

Planning for Executive Transition *77*

Recruiting and Retaining Key Financial Reporting Positions *38*

Use of, and Reliance on, Evolving Technologies

Analyzing Risk for Information Technology *66*

Analyzing Risks from External Factors *68*

Automating Balance Sheet Reconciliations *90*

Capturing Information through Electronic Data Interchange *117*

Data Capture and Processing for the Purchasing and Payables Cycle *120*

Establishing Logical Security *98*

Evaluating Business Activities to Identify Information Requirements *115*

Evaluating Financial Close End-User Spreadsheet Control Activities *95*

Identifying and Classifying Data for Financial Reporting *123*

Managing Changes to Custom Software *100*

Managing Changes to Packaged Software *99*

Obtaining a Report on Controls at
a Service Organization from a Cloud-Based Service Provider *96*

Using a Data Warehouse to Facilitate Access to Information *119*

Using Automated Tools to Enforce the Segregation of Incompatible Functions *92*

Using Governance, Risk, and Compliance Technology to Manage Internal Controls *126*

Using Technology to Identify Trends *146*

Validating Data and Information *122*

Varying Control Activities in an SDLC Based on Risk *101*

Expectations Relating to Preventing or Detecting Fraud

Assessing Fraud Risk *71*

Assessing the Potential of Management Override *30*

Cascading Responsibilities throughout the Organization and Measuring Results *44*

Conducting Ethics Audits *19*

Conducting Senior Financial Officer Visits *147*

Employee Ethics Hotline *129*

Evaluating Misconduct Reported through an Anonymous Hotline *20*

Identifying and Analyzing Risk of Material Omission and Misstatement Due to Fraud 73

Reporting Deficiencies to the Board *154*

Taking Action when Deviations Occur *21*

B: Public Comment Letters

A draft of the *Compendium* was issued for public comment from September 18, 2012, through December 4, 2012. There were twenty-three public comment letters and twenty-five responses to COSO's online survey. Each comment letter was considered by PwC and the COSO Board in finalizing this publication. This appendix summarizes the more significant issues that arose from these comment letters and the related revisions made to the *Compendium*.

Some respondents concurred with COSO that the *Compendium* provides useful illustrations of applying the *Framework* in an external financial reporting context. Some respondents expressed a view that the *Compendium* would not set a higher threshold for attaining effective internal control over external reporting or impose additional burdens on entities that report on internal control over external financial reporting.

Some agreed that the *Compendium* applies to both larger and smaller entities; however some requested additional examples specifically focused on smaller entities. PwC and the COSO Board note that many examples were obtained and updated from the COSO Guidance for Smaller Public Companies issued in 2006 and believe that most examples included in the *Compendium* apply to both larger and smaller entities.

Some respondents provided suggestions to clarify specific examples and requested additional examples. PwC and the COSO Board balanced these requests with comments provided by others that the *Compendium* is too large and included too many examples. Accordingly, a limited number of examples relevant to the application of principles in an ICEFR context were added, including:

- Reviewing Governmental Agency Financial Results and Underlying Internal Control
- Manually Assessing Incompatible Functions Across an Entity
- Reviewing Financial Statement Estimates
- Investigating and Reporting Whistle-Blower Allegations
- Identifying and Protecting Financial Data and Information
- Identifying and Analyzing Risk of Material Omission and Misstatement Due to Fraud

Additionally, the Introduction has been updated to include further discussions about:

- Limitations of Illustrations
- Objectives Established for External Financial Reporting
- Suitable Objectives of Financial Statements for External Purposes
- Risks to Achieving Suitable Objectives
- Risk Response