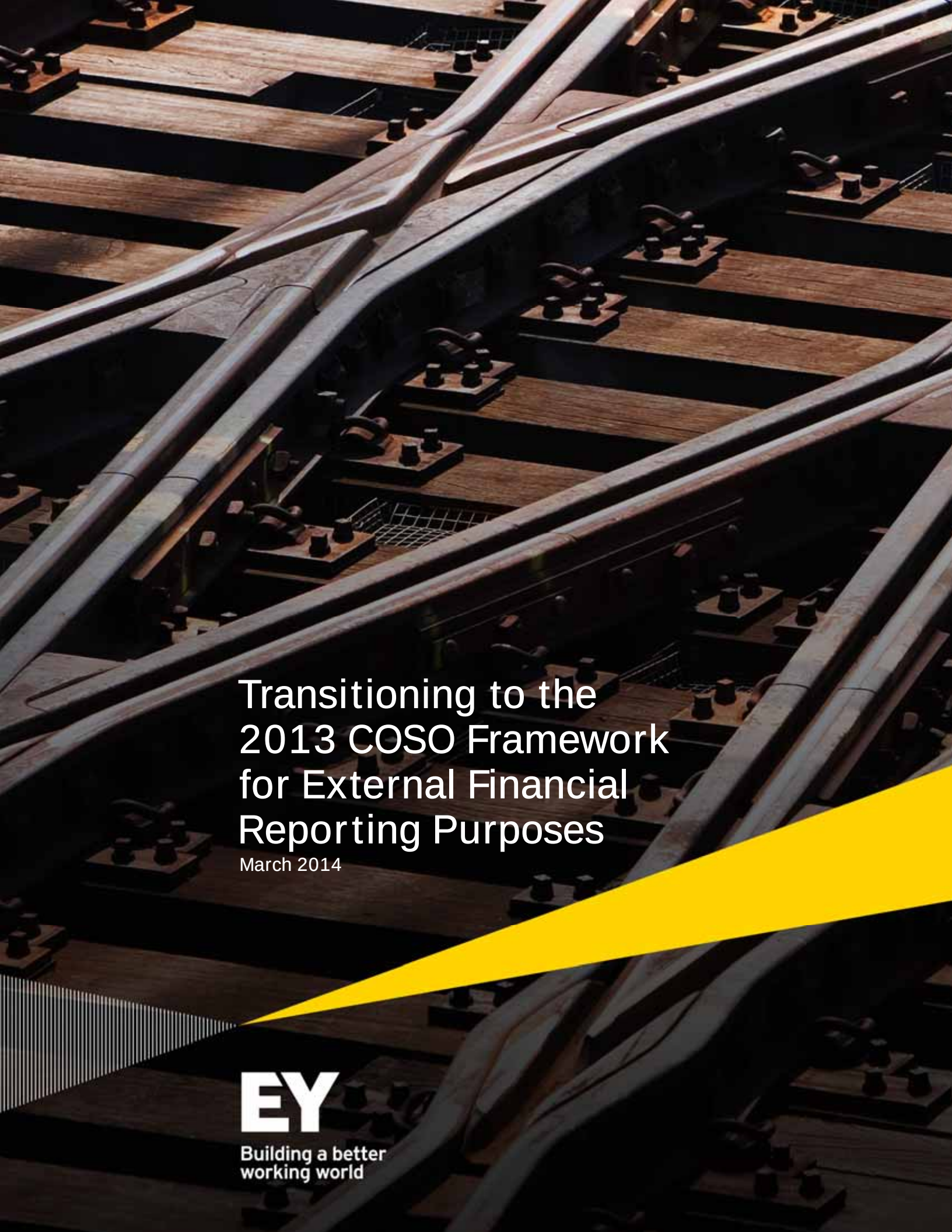
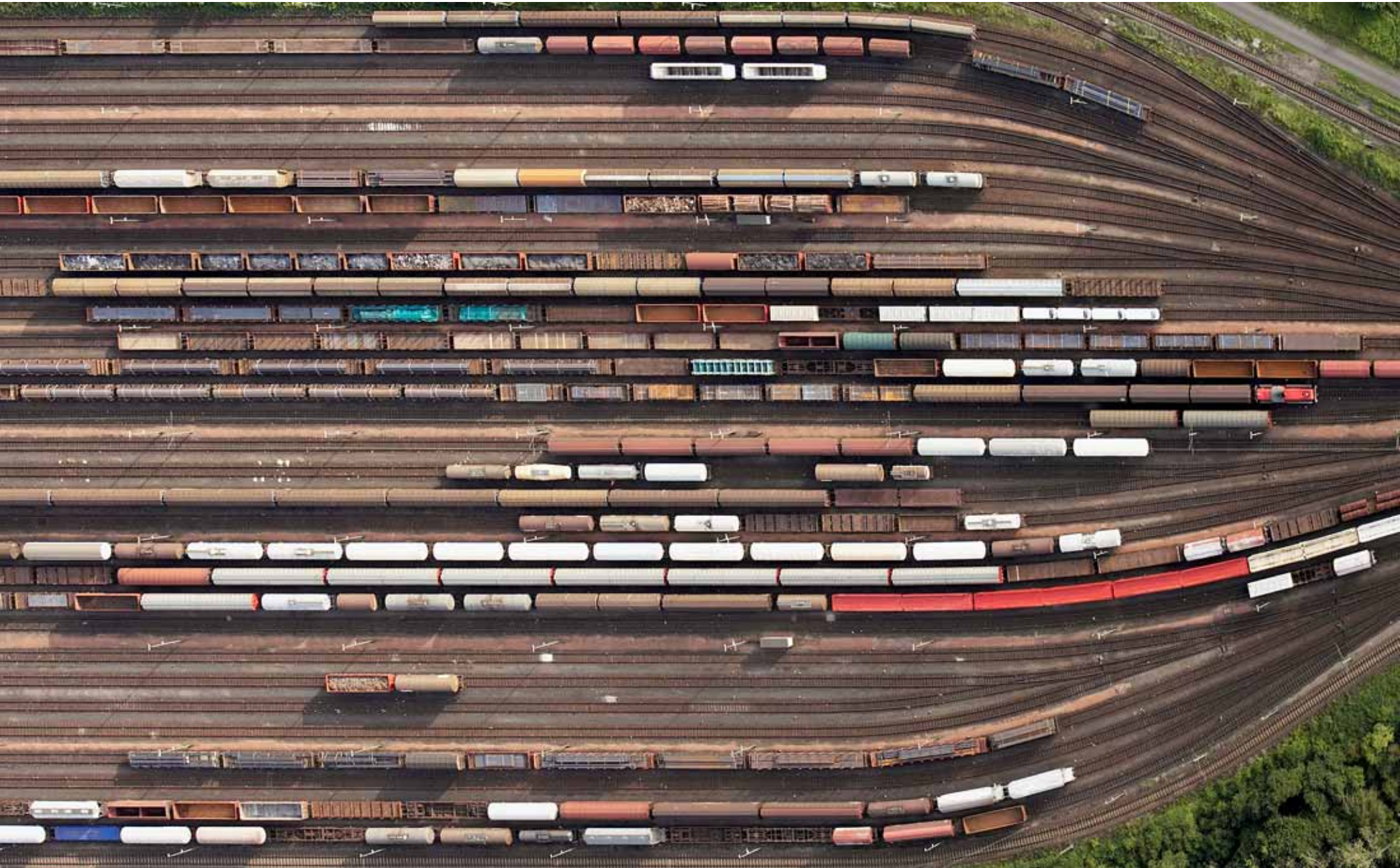


Transitioning to the 2013 COSO Framework for External Financial Reporting Purposes

March 2014

EY

Building a better working world



Introduction

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) has updated the internal control framework that many organizations use to assess internal control over financial reporting to address changes in the business, operating and regulatory environment since it issued its original framework in 1992. We believe that the structure and rigor of COSO's 2013 *Internal Control – Integrated Framework* (the 2013 framework) will increase transparency and accountability in an organization's process of designing and implementing a system of internal control.

Since the release of the 2013 framework, we have received many questions including:

- Why was the original framework updated?
- What's changed from the original framework?
- What, if anything, will organizations need to do differently?
- How much of an effort will it take to transition to the 2013 framework?
- When will my organization need to adopt the 2013 framework?

This publication addresses these and other questions that may arise during the transition. In this publication, we provide considerations for making the transition to the 2013 framework, including a suggested project plan. We have also included a questionnaire that organizations can use to evaluate whether they have addressed the important elements of the 2013 framework, as well as an example generic documentation template that can be used to help evaluate whether there may be gaps in their existing system of internal control when compared to the requirements of the 2013 framework.

Documents Released by COSO:[1]

- *Internal Control – Integrated Framework Executive Summary.* Provides a high-level overview that is intended for the board of directors, chief executive officer, and other members of senior management.
- *Internal Control – Integrated Framework and Appendices.* Defines internal control, describes requirements for effective internal control, including components and relevant principles, and provides direction for management to use in designing, implementing and conducting internal control and in assessing effectiveness; the appendices provide additional reference material but are not considered part of the 2013 framework
- *Internal Control – Integrated Framework Illustrative Tools for Assessing Effectiveness of a System of Internal Control.* Provides templates and scenarios that may be useful in applying the framework
- *Internal Control – Integrated Framework Internal Control over External Financial Reporting:* Provides practical approaches and examples that illustrate how the components and principles set forth in the framework can be applied in designing, implementing and assessing internal control over external financial reporting

[1] COSO's 2013 Framework and related materials are available at www.coso.org

As organizations begin to develop their transition plan, there are two things that we believe are important to keep in mind:

- All key stakeholders, including management and members of the board of directors, should recognize that the 2013 framework does not require an organization to redesign a system of internal control that is currently effective. However, the process of adopting the 2013 framework may identify gaps in the organization's system of internal controls where controls and/or documentation needs to be added or improved. The transition to the 2013 framework also presents opportunities for organizations to challenge their current internal control system and make enhancements and/or rationalize approaches.
- Many organizations haven't reconsidered the mapping of their system of internal control to the COSO framework since their first annual assessment required by Section 404 of the Sarbanes-Oxley Act of 2002 (SOX). This also may have been the last time an organization performed a complete review of the documentation of its systems, procedures and controls, and how it aligns with the requirements of the original framework. While the fundamental elements of the framework remain the same, organizations should use the 2013 framework to consider whether any changes are needed in their internal controls and/or related documentation. The extent of these efforts will vary depending on how extensive an organization's periodic assessments have been and the condition of its existing internal control documentation.

Public companies that use the original framework to assess the effectiveness of their internal control over financial reporting need to begin developing their plan to transition to the 2013 framework. As part of its release of the 2013 framework, COSO indicated that it will consider the original framework superseded as of 15 December 2014. The SEC staff has encouraged organizations to consider COSO's transition guidance and make the transition to the 2013 framework as soon as feasible. The SEC staff also has indicated that it plans to monitor the transition and that the longer a public company continues to use the original framework after COSO's transition date, the more likely it is that it will receive questions from the SEC staff regarding its continued use.

We have developed this publication for use by public companies that have internal control assessment responsibilities pursuant to Section 404 of SOX. While this guide may be helpful to organizations using the 2013 framework for other purposes, readers should understand that it was not developed with other objectives in mind. In addition, no publication can anticipate all possible considerations that may be relevant to the evaluation of an organization's system of internal control. Therefore, this guide should only be used to supplement the requirements and related guidance in the 2013 framework (including the related accompanying illustrative documents).

Why was the framework updated, what changed and what didn't?

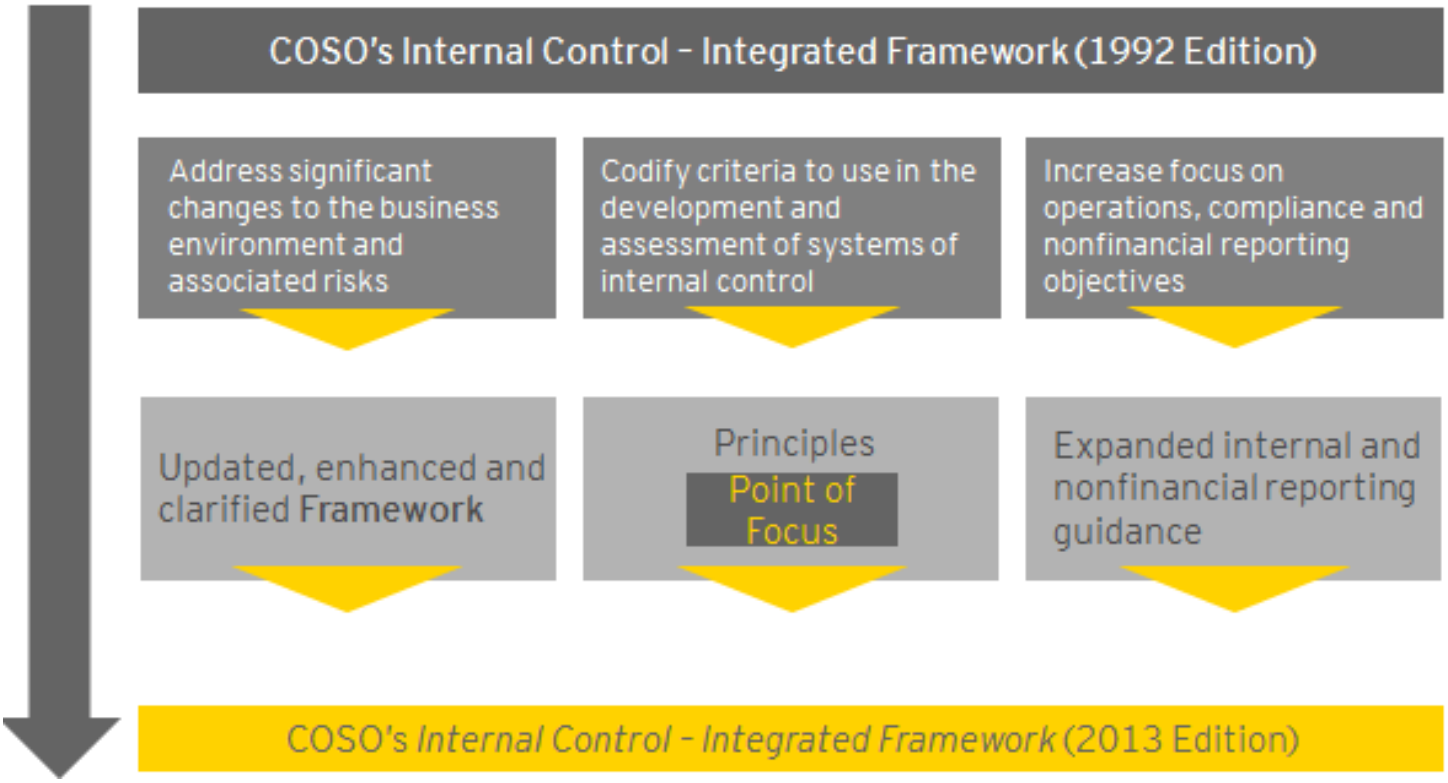
Since the release of the original framework, businesses have become increasingly complex, technologically driven and more global in scope. Stakeholders are more engaged in the business and are seeking greater transparency and accountability for the integrity of internal control that supports business decisions and governance.

COSO's enhancements to the 2013 framework are intended to (1) address significant changes in the business environment and associated risks; (2) specify criteria to use in the development and assessment of internal control; and (3) increase the focus on operations, compliance and nonfinancial reporting objectives.

What has stayed the same

It's important to recognize that a number of the core concepts of the original framework haven't changed. The 2013 framework retains the following concepts from the original framework:

- The five components that are required for an effective system of internal control:
  - Control environment
  - Risk assessment
  - Control activities
  - Information and communication
  - Monitoring activities
- The three categories of objectives of internal control:
  - Reporting[2]
  - Effectiveness and efficiency of operations
  - Compliance with laws and regulations
- The importance of judgment in designing and implementing internal control and in assessing its effectiveness



[2] While the 2013 Framework retains the "Reporting" objective from the original framework, it was expanded to include additional types of reporting, such as internal and non-financial reporting.

Definition of internal control

Internal Control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance.[3]

While the core definition of internal control has not changed, it is important to recognize that the definition emphasizes these important features of internal control:

- Internal control is a process: Internal control is constantly evolving and changing. Once implemented, internal control requires monitoring and reengineering because an organization's external and internal environments change, previously identified threats are mitigated and new risks arise.
- People are a crucial element of strong internal control: The 2013 framework makes everyone, including the members of the board of directors, management and employees, responsible for internal controls. If employees or management consistently ignore or circumvent internal controls, an organization will less likely be successful in providing effective operations, reliable financial statements or legal compliance, regardless of the effectiveness of the design of its internal controls.
- Provides reasonable assurance: An effective system of internal control can only be expected to provide reasonable, not absolute, assurance that an organization will meet its objectives.
- Internal control has four main objectives: Internal control is essential to a well-managed, well-functioning entity. Effective internal control enables the organization to do all of the following:
  - Accomplish its mission and reach its objectives
  - Produce accurate, reliable data for decision-making by management and the members of the board
  - Comply with statutes, laws and policies
  - Safeguard its assets

[3] 2013 Framework, *Glossary*

What is different?

The 2013 framework includes many enhancements and updates. One of the biggest changes is the articulation of the 17 principles that are concepts underlying the five components. While the original framework implicitly reflected these underlying principles, the 2013 framework explicitly states each principle and requires that all 17 principles be present and functioning[4] to have effective internal control.

To help organizations understand the 17 principles, COSO included "points of focus" in the 2013 framework. These points of focus are intended to help organizations design, implement, conduct and assess whether the relevant principles are present and functioning. However, while the 2013 framework establishes that the 17 principles need to be present and functioning in an effective system of internal control, organizations are not required to demonstrate that all of the points of focus are present and functioning.[5]

[4] Present refers to the determination that components and relevant principles exist in the design and implementation of the system of internal control. Functioning refers to the determination that they exist in the operation and conduct of the system of internal control. (2013 framework, *Glossary*)

[5] *2013 framework*, page 24

Other enhancements to the 2013 framework include:

- Clarifying requirements for effective internal control: For an organization to conclude that its internal control is effective, the 2013 framework requires that (1) each of the five components of internal control and relevant principles are present and functioning and (2) the five components are operating together in an integrated manner.
- Clarifying the role of objective setting in internal control: Like the original framework, the 2013 framework states that objective setting is a management process and not part of the system of internal control. The 2013 framework clarifies that the process of setting objectives is a pre-condition to the design and implementation of an effective system of internal control.
- Reflects the increased relevance of technology: Technology has evolved from large standalone mainframe environments to highly sophisticated, decentralized and mobile applications involving multiple real-time activities that can cut across many systems, organizations and processes, and can affect how all components of internal control are implemented. In recognition of technology's pervasive impact on systems of internal control, the 2013 framework includes a principle specifically focused on the role of technology as part of an organization's control activities. The 2013 framework also discusses how technology can be used to facilitate other areas of internal control.
- Enhances governance concepts: The 2013 framework expands the discussion of governance relating to the board of directors and committees of the board, including audit, compensation and nomination/governance committees.
- Considers different business models and organizational structures: The 2013 framework more prominently discusses an organization's use of external parties (such as outsourced service providers and joint venture partners) and states explicitly that the use of such third parties can extend the organization's system of internal control.
- Expands the reporting category of objectives: The financial reporting objective category is expanded to consider other types of reporting, such as nonfinancial reporting and internal financial reporting. This expansion does not affect an organization's assessment of the effectiveness of its internal control over external financial reporting pursuant to SOX. However, consideration of the elements of the 2013 framework may be helpful as organizations consider improvements to their existing internal financial or nonfinancial reporting, or consider providing stakeholders with additional information, such as sustainability reports.
- Enhances focus on risk of fraud: The 2013 framework considers risks related to fraud significant enough to warrant their own principle. It requires consideration of various types of fraud (fraudulent reporting, possible loss of assets and corruption) in the context of incentives and pressures, opportunities, and attitudes and rationalizations.

Transition

While the fundamental concepts of the original framework haven't changed, organizations should consider whether any changes are needed in their internal controls, their documentation of those controls or their annual assessment process. At a minimum, organizations adopting the 2013 framework will need to evaluate whether their existing system of internal control addresses the elements of the 2013 framework and update their existing documentation to demonstrate compliance with the 17 principles. The following discussion, and the questionnaire in Appendix A, are intended to help organizations making the transition.

Organize a Project Team to Conduct the Evaluation

Given the integral roles management, the audit committee, internal audit and other risk management functions play in an effective system of internal control, a coordinated approach to addressing the key changes in the COSO framework is important to an effective and efficient transition. The amount of effort required to make the transition will depend on an organization's size, the complexity of its operations and the quality of both its internal control and the documentation of its system of internal control. We recommend that organizations consider the following steps:

- Organize a project team with relevant parties, including management, internal audit, other risk management functions and the audit committee, as necessary, to familiarize themselves with the 2013 framework and consider the key changes and implications for the organization's system of internal control
- Undertake a process to map existing activities, controls and other documentation to the 2013 framework's five components and 17 principles. An example generic documentation template is included in Appendix B.

- Evaluate whether there are any gaps or deficiencies in activities, controls or documentation by evaluating whether the mapped controls address the elements of each of the 17 principles. A sample questionnaire for evaluating important elements of each of the 17 principles from the 2013 framework is included in Appendix A.
- Identify additional controls or enhancements to existing controls, if any, to address the identified gaps
- Update internal control documentation, and the organization's internal control annual assessment and testing plan, to help the organization evaluate whether controls are present and functioning to address the framework's 17 principles
- Evaluate any deficiencies identified

When performing these steps, many organizations may be able to prepare a single analysis that links their existing system of internal control to the key concepts of the 2013 framework. However, larger organizations that have multiple locations or multiple lines of business or operate on a decentralized basis may find it more appropriate to perform a separate evaluation for each business component and use those results in making an overall assessment at the entity level.

Key areas of focus

As part of an organization's transition plan, we believe that further consideration of the following areas may be helpful.

- Fraud risk assessment – While organizations have long considered fraud risks as part of their assessment, the focus on fraud risks in the 2013 framework (Principle 8) has led many organizations to challenge whether they need to enhance their processes to identify risks of financial statement fraud and design and implement controls that address those risks.
- Information quality – Principle 13 highlights the need to obtain or generate and use relevant quality information to support the functioning of internal control. This requires management to identify and define information requirements. While many view this principle as an extension of an organization's IT general controls, we believe that using "quality" information is fundamental to the operation of all of the 17 principles. For example, if a review control relies on certain data and reports that are used in the execution of the review control, an organization needs to have controls in place to ensure the accuracy and completeness of those data and reports.
- Consideration of different business models and organization structures – Due to changes in how businesses operate and address their technology needs, the risks presented by various business models and organizational structures (e.g., service organizations, offshore centers, business partners, joint ventures) are given more attention in the 2013 framework. The 2013 framework reinforces the concept that regardless of whether aspects of an organization's processes and/or functions are provided by an outside party, management is responsible for the sufficiency of the controls and their effective operation.
- Deficiency evaluation – As mentioned previously, the 2013 framework notes that an effective system of internal control is one in which (1) all five of the components and relevant principles are present and functioning and (2) the five components operate together in an integrated manner. As a result, organizations will need to consider and evaluate deficiencies in the context of the 17 principles.

Use of this resource

We have developed the following sample tools organizations may leverage to evaluate and document their system of internal control using the 17 principles in the 2013 framework:

- 2013 Framework Questionnaire: probing questions and key concepts (Appendix A). This list of questions may be used to evaluate whether existing systems of internal control address key concepts for each of the 17 principles in the 2013 framework. It is primarily intended for use by organizations that have previously evaluated the effectiveness of their internal control over financial reporting under SOX. However, organizations performing an evaluation for the first time may also find it helpful.
- Example documentation template (Appendix B): This generic template may be used by organizations to link their existing internal controls to the 17 principles and identify any gaps.

Summary

Transitioning to COSO 2013 will require incremental effort, more for some organizations than others. Organizations should get an early start so that the transition can be thoughtful and the benefits of an effective system of internal control can be fully realized. As always, we would be pleased to discuss the evaluation of internal control over financial reporting with you, and provide our advice where appropriate.

Appendix A – 2013 Framework Questionnaire: Probing Questions and Key Concepts

This questionnaire was developed for consideration by management in its transition from COSO's original framework to the 2013 framework.

Many organizations may be able to prepare a single analysis the supplements the questionnaire that links its existing system of internal control to the key concepts of the 2013 framework. However, larger organizations that have multiple locations or multiple lines of business and/or operate on a decentralized basis may find it more appropriate to perform a separate evaluation for each business component and use those results to make an assessment at the entity level.

We have listed several questions for each of the 17 principles. This list is not all-inclusive, and not all of the questions apply to every organization. An organization's facts and circumstances may give rise to additional questions to consider as part of its transition.

While a "no" response to a single question does not necessarily mean that a principle is ineffective, it could indicate areas where management should focus attention (particularly when there are several "no" responses). The "Reference" column, as well as the example generic documentation template in Appendix B, was created to assist in linking an organization's existing controls documentation to each of the relevant areas within each principle.

While this list was primarily developed to provide considerations related to internal controls over financial reporting at the entity level, many of the questions are relevant to the evaluation of the design of controls at the process/transaction level. For example:

- Principles 10 through 12 – The organization should consider whether it has identified and implemented control activities that are designed to address the identified financial reporting risks. Such controls include automated controls that are supported by relevant IT general controls.
- Principle 13 – In evaluating the design of controls at the process/transaction level, management should consider whether (1) it has identified the information necessary to support the operation of controls as intended and (2) whether it has adequate controls in place to obtain or generate quality information to support the functioning of the controls.

As a result, organizations should generally consider each of the above for controls that address financial reporting risks at the process/transaction level (i.e., for controls that address risks for each relevant assertion, related significant accounts or disclosures and underlying processes) as part of the evaluation of their design and operation.

Control Environment

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

		Yes	No	Reference
Principle 1: The organization demonstrates a commitment to integrity and ethical values.				
1.1	Is the board of directors and management's commitment to integrity and ethical behavior communicated effectively throughout the organization, both in words and deeds? Do the board of directors and management lead by example?	☐	☐	
1.2	Is the tone set by the board of directors and senior management communicated through to various operating units? Do such communications consider the various factors, including potential barriers, that may be present at each unit (e.g. cultural, language)?	☐	☐	
1.3	Is the tone exhibited by management of operating units consistent with that set by the board of directors and senior management?	☐	☐	
1.4	Is there a code of conduct and/or ethics policy and has it been adequately communicated to all levels of the organization?	☐	☐	
1.5	If there is a code of conduct, does it provide standards to guide the organization's behaviors, activities and decisions by doing the following things? • Establishing what is right and wrong? • Reflecting local laws, rules, regulations, standards and other expectations that the organization's stakeholders may have • Meeting the specific needs of various operating units (e.g. based on market, culture, language) so it can be consistently implemented throughout the organization?	☐	☐	
1.6	Is the organization's commitment to integrity and ethical behavior regularly communicated to joint venture partners, suppliers, sales distributors, outsourced service providers and other business partners?	☐	☐	
1.7	Are those in top management hired from outside made familiar with the importance of high ethics and controls?	☐	☐	
1.8	Is the organization's commitment to integrity and ethical behavior included in training for new employees and contractors?	☐	☐	
1.9	Does the organization have a process in place to communicate standards of conduct throughout the organization, including external partners/outsourced service providers?	☐	☐	
1.10	Does the organization have a process to evaluate the performance of individuals and teams against its standards of conduct? Does it consist of the following: • Continual and periodic compliance procedures • Consideration of integrity and ethical values in performance reviews, compensation and promotion decisions • Investigation of allegations of noncompliance of its standards of conduct by independent personnel	☐	☐	

		Yes	No	Reference
1.11	Has the organization established tolerance levels for deviations to its standards of conduct? Are such tolerance levels communicated throughout the organization? Are deviations evaluated in a timely manner?	☐	☐	
1.12	Does the organization periodically analyze issues to identify trends and root causes to evaluate whether modification of policies, communication, training or controls are necessary?	☐	☐	
Other		☐	☐	
Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.				
2.1	Is the makeup of the board of directors, including the number of directors and their background and expertise, appropriate given the nature of the organization? Are the makeup and skills of the board members periodically evaluated to assure that directors have the expertise to ask probing questions of management and to take appropriate actions?	☐	☐	
2.2	Has the independence of outside board members been adequately reviewed, including affiliations and relationships and transactions with the organization or other organizations that could result in a conflict of interest?	☐	☐	
2.3	Is the expertise of the board members evaluated on a regular basis?	☐	☐	
2.4	Do board members participate in training as appropriate to keep their skills and expertise current and relevant?	☐	☐	
2.5	Does the audit committee have a charter outlining its duties and responsibilities? Does the audit committee have adequate resources and authority to discharge its responsibilities	☐	☐	
2.6	Is the board of directors or audit committee an informed, vigilant and effective overseer of the financial reporting process and the organization's internal control, including technology and relevant risks and controls, covering all five components of internal control?	☐	☐	
2.7	Does the board of directors or audit committee maintain a direct line of communication with the entity's external and internal auditors?	☐	☐	
2.8	Does the board of directors or the audit committee stay abreast with current internal control practices in the entity as well as the industry, and is it aware of recent regulations and changes that affect the overall system of internal control at the organization?	☐	☐	
Other		☐	☐	

		Yes	No	Reference
Principle 3: Management establishes, with board oversight, structures, reporting lines and appropriate authorities and responsibilities in the pursuit of objectives.				
3.1	Is the organizational structure appropriate for the size, operating activities and locations of the organization to enable management to carry out their oversight responsibilities?	☐	☐	
3.2	Does management review and make modifications to the organizational structure of the organization in light of changed conditions or revised priorities?	☐	☐	
3.3	Are the reporting lines clear and appropriate to enable accountability over operating units and functional areas? Are reporting lines evaluated periodically, and do they enable the execution of authorities and responsibilities and the flow of information to manage the entity's activities?	☐	☐	
3.4	Are job descriptions that outline financial reporting responsibilities maintained and updated when necessary?	☐	☐	
3.5	Are there adequate policies and procedures for authorization and approval of transactions by the appropriate level?	☐	☐	
3.6	Is there an appropriate structure for assigning ownership of data, including who is authorized to initiate and/or change transactions? Is ownership assigned for each application and database within the IT infrastructure?	☐	☐	
3.7	Is there an appropriate segregation of incompatible activities (i.e., separation of accounting for and access to assets) both physically and through access to the IT systems?	☐	☐	
3.8	Are the contractual terms with outsourced service providers clear and concise with regard to the organization's objectives and expectations of conduct and performance, competence levels and expected information and communication flow?	☐	☐	
3.9	Is assignment of responsibilities clear, including third-party service providers (who carry out activities on behalf of the organization), related to the extent of their decision-making rights?	☐	☐	
3.10	Are there appropriate policies for matters such as accepting new business, conflicts of interest and security practices? Are they adequately communicated throughout the organization?	☐	☐	
Other		☐	☐	
Principle 4: The organization demonstrates a commitment to attract, develop and retain competent individuals in alignment with objectives.				
4.1	Are there standards and procedures for hiring, training, motivating, evaluating, promoting, compensating, transferring and terminating the employment of personnel that are applicable to all functional areas?	☐	☐	
4.2	Are there screening procedures for job applicants?	☐	☐	

		Yes	No	Reference
4.3	Does the organization have policies and practices in place to articulate the skills, competencies and behaviors that should be place at all levels of the organization, including outsourced service providers?	☐	☐	
4.4	Are there written job descriptions, reference manuals or other forms of communication to inform personnel of their duties?	☐	☐	
4.5	Does management demonstrate a commitment to provide sufficient accounting and financial personnel to keep pace with the growth and/or complexity of the business?	☐	☐	
4.6	Are training needs identified and delivered to requisite personnel to address needs such as emerging standards or other areas where improvement is needed?	☐	☐	
4.7	Does management set expectations that personnel raise issues or questions relating to significant financial reporting or internal control issues?	☐	☐	
4.8	Does the organization have policies and practices that include executing and evaluating performance, including taking remedial actions for any issues identified?	☐	☐	
4.9	Are there periodic evaluations of departmental staffing needs (particularly with regard to knowledge and experience of management and supervisory levels within the accounting, information systems and financial reporting areas)?	☐	☐	
4.10	Does a formal process exist to evaluate competence, identify gaps and document specific and measurable remediation plans to address underlying risks and root cause linked to incompetence, training, motivation and other behavioral drivers (that result in competence issues)? Does this evaluation encompass outsourced service providers?	☐	☐	
4.11	Do the entity's policies include succession plans for senior executives and contingency plans for assignments of responsibilities important for internal control?	☐	☐	
Other		☐	☐	
Principle 5: The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.				
5.1	Does the organization's structure and tone at the top help establish and enforce individual accountability for performance of internal control responsibilities? Does it communicate and reinforce the accountability for responsible conduct of all personnel?	☐	☐	
5.2	Is there a mechanism in place to regularly educate and communicate to management and employees the importance of internal controls, and to raise their level of understanding of controls?	☐	☐	

		Yes	No	Reference
5.3	Does management have processes and controls in place to evaluate and hold outsourced service providers (and other business partners) accountable for their internal control responsibilities?	☐	☐	
5.4	Does the organization provide measures, incentives and other rewards that are aligned with ethical values and performance related to internal control, including financial and nonfinancial measures?	☐	☐	
5.5	Does management set realistic (i.e., not unduly aggressive) financial targets and expectations for operating personnel?	☐	☐	
5.6	Are performance measures reviewed periodically for relevance and adequacy in relation to their potential risks and rewards?	☐	☐	
5.7	Does the board of directors and management act to remove or reduce incentives or temptations that might prompt personnel to engage in dishonest, illegal or unethical acts?	☐	☐	
5.8	Do management and the board of directors evaluate performance of internal control responsibilities, including adherence to standards of conduct and levels of competence? Do appropriate rewards or disciplinary actions result from such evaluations?	☐	☐	
Other		☐	☐	

Risk Assessment

Risk assessment involves a dynamic and iterative process for identifying and analyzing risks to achieving the entity's objectives and forming a basis for determining how risks should be managed. In this context, risk assessment involves identifying and analyzing risks that the organization's external financial statements are not fairly presented in accordance with the requirements of the applicable financial reporting framework. As part of this process, management considers possible changes in the external environment, such as changes in the applicable financial reporting standards and within its own processes and procedures, that may impede its ability to achieve its objectives.

		Yes	No	Reference
Principle 6: The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.				
6.1	Are the external financial reporting objectives consistent with the relevant financial reporting framework and appropriate in the circumstances?	☐	☐	
6.2	Does management establish a materiality threshold for the purpose of identifying significant accounts and disclosures? Does this consider risks at all locations/geographies where the entity conducts activities?	☐	☐	
6.3	Does the organization specify objectives by identifying the following: • Significant financial statement accounts and disclosures • Relevant assertions • Underlying transactions and events • Processes supporting those accounts and disclosures	☐	☐	

		Yes	No	Reference
6.4	Do the organization's policies, procedures and processes facilitate the development of financial statements that reflect the transactions and events that underlie them? For example, do they consider: • Relevance – information that is meaningful to users of the financial statements • Faithful representation – information that is complete, neutral and free from error • Comparability – information that facilitates comparison with other entities and with similar information from the same entity • Verifiability – information that can be substantiated • Timeliness – information that can be provided in time to be useful to users of the financial statements • Understandability – information that is presented clearly and concisely	☐	☐	
6.5	Does the organization consider the factors in 6.4 above when establishing accounting policies where alternative treatments under the relevant financial reporting framework may exist?	☐	☐	
6.6	Does the organization periodically review and update its understanding of the requirements of the applicable financial reporting framework?	☐	☐	
6.7	Does the organization have a process to evaluate the range of its activities to assess whether all material activities are appropriately reflected in the financial statements?	☐	☐	
Other		☐	☐	
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.				
7.1	Does the organization identify risks to the achievement of financial reporting objectives at all levels of the entity (e.g. subsidiary, division, operating unit and functional levels)?	☐	☐	
7.2	Does the organization's process to identify risks to the achievement of financial reporting objectives include consideration of both internal and external risk factors to each significant financial statement account or disclosure, and related assertions? Consider the following: • Quantitative and qualitative factors • Nature of account, such as volume of transactions, complexity and degree of judgment required to determine amount or disclosure • Nature of the underlying class of transactions, including whether such transaction streams are centralized or decentralized, the IT applications used, whether the transactions are subject to changes during the year, and the level of involvement and/or interaction with external parties • Risks associated with the accounting and reporting for infrequent and/or unusual transactions for which controls may not have been implemented in the normal course of business	☐	☐	

		Yes	No	Reference
	• Whether fraud risks are associated with the particular account or disclosure • Whether a new financial reporting standard or law or regulation exists that requires different or additional reporting • Impact of changing user needs or expectations on the amounts reflected in the organization's financial statements • Changes in management responsibilities that can affect the way certain controls operate • The quality of personnel hired and the methods of training and motivation • The nature of the entity's activities and employee accessibility to assets • A disruption in information processing			
7.3	Is the risk identification comprehensive and does it include all significant interactions internal to an entity and between the entity and its relevant business partners and outsourced service providers?	☐	☐	
7.4	Does the organization involve the appropriate levels of management with the necessary expertise to identify risks to achieving its financial reporting objectives, and to perform the related assessment of the risks? For example: • Are there processes to ensure the accounting department is made aware of changes in the operating environment so they can review the changes and determine what, if any, effect the change may have on the entity's accounting policies? • Are there channels of communication between the accounting department and/or individuals in charge of monitoring regulatory rules so the accounting department is aware of regulatory changes that could affect the entity's accounting policies? • Are there processes to ensure that the accounting department (and/or audit committee) is aware of significant transactions with related parties so they can determine whether such transactions are appropriately approved, accounted for and disclosed? • Does the audit committee review and approve significant changes to the organization's accounting practices?	☐	☐	
7.5	Does management's risk assessment process consider the likelihood and magnitude of occurrence of an identified risk?	☐	☐	
7.6	Is the risk assessment revisited on an appropriate interval?	☐	☐	
Other		☐	☐	

		Yes	No	Reference
Principle 8: The organization considers the potential for fraud in assessing risks to the achievement of objectives.				
8.1	Does the organization perform a risk assessment to consider risk related to fraudulent financial reporting, management override, potential loss of assets and corruption?	☐	☐	
8.2	Does the organization's risk assessment process include an evaluation of incentives and pressures, opportunities, attitudes and rationalizations to commit fraud (e.g. reviewing incentive compensation programs to evaluate how meeting, or not meeting, financial reporting targets could provide incentives and pressures for employees to commit fraud)?	☐	☐	
8.3	Does the assessment of fraud risk consider opportunities for unauthorized acquisition, use, or disposal of assets, altering the organization's reporting records or committing other inappropriate acts?	☐	☐	
8.4	Does the assessment of fraud risk consider the opportunities for willful violations of laws or governmental regulations that could have a material direct or indirect impact on external financial reporting?	☐	☐	
8.5	Does the assessment of fraud risk consider the various ways that fraudulent financial reporting could occur? For example: • Management bias • The degree of estimates and judgments in external reporting • Fraud schemes and scenarios common to the industry sectors and markets in which the organization operates • Geographic regions where the entity does business • Incentives that may motivate fraudulent behavior • Nature of technology and management's ability to manipulate information • Unusual or complex transactions subject to significant management influence • Vulnerability to management override and potential schemes to circumvent existing control activities	☐	☐	
8.6	Does the assessment of fraud risk consider how management and other personnel might engage in or justify inappropriate actions?	☐	☐	
8.7	Does the organization have established procedures to periodically reconcile physical assets (e.g., cash, accounts receivable, inventories, fixed assets) with the related accounting records?	☐	☐	
Other		☐	☐	

		Yes	No	Reference
Principle 9: The organization identifies and assesses changes that could significantly impact the system of internal control.				
9.1	Are there groups or individuals who are responsible for anticipating or identifying external changes with possible significant effects on the entity (e.g., regulatory or economic changes)? Are there processes in place to inform appropriate levels of management about changes with possible significant effects on the entity?	☐	☐	
9.2	Does the organization consider the potential impact of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations, rapid growth, changing reliance on foreign geographies and new technologies on its system of internal control?	☐	☐	
9.3	Does the organization have a process to consider changes in management and their respective attitudes and philosophies on the system of internal control?	☐	☐	
Other		☐	☐	

Control Activities

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

		Yes	No	Reference
Principle 10: The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.				
10.1	Has the organization undertaken a process to: • Address the identified financial reporting risks via specific responses? • Consider all the relevant business processes, information technology and locations where control activities are needed (including outsourced service providers and other business partners)? • Consider control activities to address the integrity of information sent to and received from outsourced service providers? • Consider adequacy of controls performed by outsourced service providers and other business partners? For example, has management mapped controls to address each risk related to the relevant financial statement assertions?	☐	☐	
10.2	Are the appropriate personnel involved in the process of designing and implementing controls to respond to the identified risks (e.g., financial personnel, internal auditors, business process owners)?	☐	☐	

		Yes	No	Reference
10.3	Do the controls employed by the organization include authorizations, approvals, comparisons, physical counts, reconciliations and supervisory controls?	☐	☐	
10.4	Are the controls employed by the organization appropriate based on the organization's environment, complexity, nature, scope and characteristics, as well as those of the particular business process?	☐	☐	
10.5	Do the controls include a range and variety of controls, including manual and automated, preventive and detective?	☐	☐	
10.6	Do the controls identified address the completeness, accuracy and validity of transactions processed?	☐	☐	
10.7	Do the controls identified include controls over the completeness, accuracy and validity of reference data used in transaction processing (e.g. a pricing master file) and the operation of other controls (e.g. reconciliation controls)?	☐	☐	
10.8	Has the organization considered the precision (i.e., the degree to which controls, if operating effectively, would prevent or detect misstatements in the financial statements that could be material) of the controls when evaluating the extent to which they address the identified risks? For example, have they considered the following: • Whether the level of precision objective (system-based) or subjective (performance of a review) • The nature of errors identified by the control • Whether there is adequate follow-up in response to discrepancies or errors identified • What evidence exists to confirm the control operated as intended	☐	☐	
10.9	Do controls exist at various levels within the organization from transaction level controls to entity-level management review controls?	☐	☐	
10.10	Is there appropriate segregation of duties (e.g., separation of accounting for and access to assets, IT operations function separate from systems and programming, database administration function separate from application programming and systems programming)? Are organizational charts, automated tools, process flow diagrams or other tools used to ensure proper segregation of duties exist?	☐	☐	
10.11	Are appropriate approvals from management required prior to allowing an individual access to specific applications and databases?	☐	☐	
10.12	Are IT personnel prohibited from having incompatible responsibilities or duties in user departments?	☐	☐	
10.13	Are there processes to periodically (e.g., quarterly, semiannually) review system privileges and access controls to the different applications and databases within the IT infrastructure to determine whether system privileges and access controls are appropriate?	☐	☐	
Other		☐	☐	

		Yes	No	Reference
Principle 11: The organization selects and develops general control activities over technology to support the achievement of objectives.				
11.1	Are there processes in place to select, develop, operate and maintain the organization's technology? Are they appropriate for the nature and extent of the technology used?	☐	☐	
11.2	Has the organization identified each system that performs a role in the processing of transactions underlying significant accounts or disclosures and established IT general controls over those systems?	☐	☐	
11.3	Does the organization have controls over program acquisition, implementation and maintenance? If so, consider: • Whether formal policies and procedures are in place that define an approach to systems acquisition and change management (e.g., a formal systems development methodology) • Whether user department and IT department management approval is required before systems acquisition and change projects are undertaken • Whether the IT department maintains project documentation, including systems requirements definitions, risk analyses and cost-benefit analyses • Whether the systems acquisition and change management approach addresses security risks • Whether the systems acquisition and change management approach addresses data conversion • Whether environments for development (or modification) and testing of IT solutions are separated (either logical or physical) from production systems • Whether users are actively involved in the test process • Whether development personnel are prohibited from migrating applications and data from the test environment to production • Whether post-implementation review procedures are performed for system modifications made during an emergency	☐	☐	
11.4	Do policies and procedures exist and are they followed with regard to obtaining and implementing patches to the operating system, database and application software?	☐	☐	
11.5	Does the organization have controls over access to IT systems? If so consider: • Whether formal policies and procedures are in place that define an approach to system security (including confidentiality of data and information) • Whether a mechanism is in place for communicating security policies to employees (e.g., requiring users to sign an acknowledgement that they have read and understood the organization's security policies) • Whether a security organization exists that is independent of both the user departments and other IT department functions	☐	☐	

		Yes	No	Reference

	• Whether IT department personnel do not have operational or accounting responsibilities
	• Whether appropriate user department and IT department management control access to the following:
	  • Entity networks
	  • Remote connection to networks and/or applications
	  • Internet/intranet sites
	  • Applications and application modules
	• Whether the following user account security parameters are in place:
	  • Users are assigned unique user IDs
	  • Adequate passwords are required (e.g., minimum and maximum password length, at least one alpha and one numeric character)
	  • Periodic password changes are required
	  • User accounts are disabled after a limited number of unsuccessful logon attempts
	  • Users are limited to one session per account (e.g., concurrent sessions or logons are not allowed)
	  • Measures are in place to prevent the repeated use of a password
	  • Administrator rights are assigned to a limited number of individuals who require those rights to perform their job duties
	• Whether system security settings are configured to protect the entity's information
	• Whether documented standards exist and are followed for the setup of new servers
	• Whether access to security settings is limited to appropriate IT personnel
	• Whether communications with public networks are controlled by a firewall. The firewall is implemented to:
	  • Hide the structure of the client's network
	  • Provide an audit trail of communications with public parties
	  • Generate alarms when suspicious activity is suspected
	  • Defend itself and/or the organization's network against attack
	• Whether procedures for protection against malicious programs are in place through the use of anti-virus software and other measures (which may include policies limiting the installation of unapproved programs, procedures for reporting suspected occurrences of viruses, etc.)
	• Whether physical access to technology infrastructure is restricted
	• Whether access to internal networks and/or applications by suppliers, customers, and/or other business partners is approved by appropriate management and limited to those networks and/or applications required to conduct business
	• Whether representatives of suppliers, customers and/or other business partners are required to adhere to the client's policies, procedures, and security standards when accessing the client's systems			

		Yes	No	Reference
11.6	Do the IT general controls identified appropriately consider the technology infrastructure in use (e.g., backups of applications, databases and operating systems are performed at appropriate intervals and periodically tested for recoverability)?	☐	☐	
11.7	Are responsibilities clear for initiating processing jobs (including subsequent checking for full completion) relating to internal transactions (e.g., invoicing) and the loading of third-party information (e.g., pricing data)?	☐	☐	
11.8	Are the IT general controls identified appropriate to address the risks posed by complete system replacement or extensive revision, where relevant?	☐	☐	
11.9	Has the organization identified appropriate technology controls to address the risks of using applications hosted by third-parties?	☐	☐	
Other		☐	☐	
Principle 12: The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.				
12.1	Has the organization developed and documented policies and procedures for all significant financial statement accounts and disclosures? For example: • Rationale for the policy, including risks to the financial statements • Locations, units and processes to which the policies relate • Clearly established responsibilities and accountability related to the execution of a particular policy/procedure, including the precision by which the policy/procedure is intended to operate • Corrective actions to be taken as part of performing the activity • Procedures for follow-up on exceptions identified • Skills and level of authority required of person(s) performing the control • Expectations regarding timeliness of performance of a control and any necessary follow-up • Expectations for the documentation/evidence required to be maintained to support performance of the control	☐	☐	

		Yes	No	Reference
12.2	Do the entity's policies and procedures include the following: • Accounting and closing practices that are followed consistently at interim dates (e.g., quarterly, monthly) throughout the year? • Is there appropriate involvement by management in reviewing significant accounting estimates and support for significant unusual transactions and non-standard journal entries? • Is there timely and appropriate documentation for transactions? • Does the entity review its policies and procedures periodically to determine whether they continue to be appropriate for the organization's activities? • Does management review key performance indicators (e.g., budget, profit, financial goals, operating goals) regularly (e.g., monthly, quarterly) and identify significant variances? • Does management investigate significant variances and is appropriate corrective action taken? • Are variances in planned performance communicated and discussed with the board of directors and/or the audit committee at least quarterly? • Are financial statements submitted to operating management? Are they accompanied by analytical comments? • Has management established procedures to prevent unauthorized access to, or destruction of, documents, records (including computer programs and data files), and assets? • Is data processing access to non-data processing assets restricted (e.g., blank checks)?	☐	☐	
12.3	Does the organization review its policies and procedures periodically to determine whether they continue to be appropriate for the organization's activities and refresh them when needed?	☐	☐	
12.4	Does the organization have formal policies and procedures in place that: • Define an approach to systems acquisition and change management? • Obtaining and implementing patches to the operating system, database and application software? • Define an approach to system security (including confidentiality of data and information)?	☐	☐	
Other		☐	☐	

Information and Communication

Information is necessary for the entity to carry out internal control responsibilities to support the achievement of its external financial reporting objectives. Communication is the continual, iterative process of providing, sharing and obtaining necessary information to design, implement and conduct internal control, and to assess its effectiveness.

		Yes	No	Reference
Principle 13: The organization obtains or generates and uses relevant, quality information to support the functioning of internal controls.				
13.1	Has the organization established information requirements to support the effective operation of controls within the five components of internal control? Are such requirements at the relevant level and needed specificity to support the identification of relevant and reliable sources of information and data?	☐	☐	
13.2	Does the organization consider both internal and external sources of data when identifying relevant data to use in the operation of internal control?	☐	☐	
13.3	Does management re-evaluate its information needs periodically?	☐	☐	
13.4	Do the organization's information systems generate information that is of sufficient quality to support the effective operation of controls? For example, has management developed and implemented controls related to: • Completeness and accuracy of data • Capture of data at the necessary frequency • Providing information when needed • Protection of sensitive data • Retention of data to comply with relevant business, audit and regulatory needs	☐	☐	
13.5	Does the organization periodically review the quality of information to assess its reliability and timeliness?	☐	☐	
13.6	With respect to information obtained from external sources, does the organization have controls to ensure: • The external sources are appropriate • Information is supported by evidence from the source • In formation is of sufficient quality to support the effective operation of the control	☐	☐	
Other		☐	☐	

		Yes	No	Reference
Principle 14: The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.				
14.1	Is there training/orientation for new employees, or employees when starting a new position, to discuss the nature and scope of their duties and responsibilities? Does such training/orientation include a discussion of specific internal controls they are responsible for?	☐	☐	
14.2	Has the organization implemented policies and procedures that facilitate effective internal communication, including individual internal control authorities and responsibilities and standards of conduct across the organization?	☐	☐	
14.3	Are there written job descriptions and reference manuals that describe the duties of personnel, including their internal control responsibilities?	☐	☐	
14.4	Does senior management communicate the organization's financial reporting objectives clearly through the organization so that other management and personnel, including non-employees such as contractors, understand their individual roles in the organization, regardless of physical location?	☐	☐	
14.5	Does the organization's messaging reinforce to all employees their roles in ensuring that internal control responsibilities are taken seriously?	☐	☐	
14.6	Is there a process to quickly disseminate critical information throughout the entity when necessary?	☐	☐	
14.7	Do communications between the board of directors and management facilitate their oversight of the organization's internal control and include, for example: • Matters important to the assessment of risks to the achievement of the organization's financial reporting objectives • Results of the organization's monitoring programs	☐	☐	
14.8	Do members of the board of directors have direct access to employees without interference from management?	☐	☐	
14.9	Does internal audit have a direct line of communication to the audit committee?	☐	☐	
14.10	Is there a process for employees to communicate improprieties? Is the process well-communicated throughout the entity? Does the process allow for anonymity for individuals who report possible improprieties? Is there a process for reporting improprieties, and actions taken to address them, to senior management, the board of directors or the audit committee?	☐	☐	
14.11	Are policies and procedures established for and communicated to personnel at decentralized locations? Has management taken into account cultural, ethnic and generational differences in determining appropriate methods of communication?	☐	☐	

		Yes	No	Reference
14.12	Is there periodic evaluation of the effectiveness of communications to ensure the methods are working?	☐	☐	
Other		☐	☐	
Principle 15: The organization communicates with external parties regarding matters affecting the functioning of internal control.				
15.1	Does the organization have processes in place to communicate relevant and timely information to external parties including shareholders, partners, owners, regulators, customers, financial analysts and other external parties?	☐	☐	
15.2	Does the organization have a process in place to approve formal external communications prior to their release?	☐	☐	
15.3	Is there a process for tracking communications from customers, vendors, regulators, and other external parties and sharing it internally?	☐	☐	
15.4	Is information from external parties about the organization's activities that relates to matters of internal control evaluated by management and, where appropriate, communicated to the board of directors or the audit committee?	☐	☐	
15.5	Does the organization have separate communication channels outside of the normal operations available to customers, suppliers and outsourced service providers to allow them to communicate directly with management and other personnel (such as a whistleblower hotline)?	☐	☐	
Other		☐	☐	

Monitoring

Monitoring consists of the activities used to ascertain whether each of the five components of internal control, including controls to address the principles within each component, is present and functioning. Findings are evaluated and deficiencies are communicated in a timely manner, with serious matters reported to senior management and to the board of directors.

		Yes	No	Reference
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.				
16.1	Does management have processes in place to assess whether controls within each of the five components of internal control are present and functioning as intended?	☐	☐	
16.2	Does the monitoring include evaluations built into business/financial reporting processes and performed on a real-time basis (ongoing evaluations) as well as separate evaluations performed periodically?	☐	☐	

		Yes	No	Reference
16.3	Does the organization's monitoring programs, including the mix of ongoing monitoring and separate evaluations and the frequency of the monitoring activities, consider the following: • Scope and nature of the organization's operations • The levels of risk throughout the entity (e.g., the level of risk by location, by business unit, by business process) • Frequency and significance of changes in the organization's operations	☐	☐	
16.4	Does the organization's monitoring activities provide for the establishment of the understanding of the design and current state of the internal control system (e.g. performance of walkthroughs)? Is that understanding updated periodically?	☐	☐	
16.5	Are the results of monitoring activities considered over time to determine the basis for future monitoring activities?	☐	☐	
16.6	Is the level of staffing, training and specialized skills of the people performing the monitoring adequate given the environment (e.g., use of experienced, trained information systems auditors in complex and highly automated environments)?	☐	☐	
16.7	Is an internal audit function used as part of the organization's monitoring program? If so: • Is it independent (in terms of authority and reporting relationships) of the activities the function audits? • Do internal auditors have direct access to the board of directors or audit committee? • Is the scope of internal audit activities appropriate given the nature, size and structure of the organization?	☐	☐	
16.8	Are there other quasi-audit functions (e.g., credit review in a financial institution or risk management in an insurance company) that report to management and affect the overall control environment?	☐	☐	
16.9	Do the monitoring activities include observations, inquiries and inspection of evidence?	☐	☐	
16.10	Are periodic assessments of the security of the IT environment performed?	☐	☐	
16.11	Are procedures in place to monitor when controls are overridden and to determine whether the override was appropriate?	☐	☐	
16.12	Do the organization's monitoring activities consider services performed by outsourced service providers?	☐	☐	
Other		☐	☐	

		Yes	No	Reference
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.				
17.1	Is there a process in place to accumulate and evaluate matters identified by the organization's monitoring activities? Does this process include consideration of any themes underlying the identified deficiencies as well as potential root causes?	☐	☐	
17.2	Does the organization receive findings and recommendations from external parties such as regulators, customers, vendors and external auditors? Is there a process in place for evaluating these matters?	☐	☐	
17.3	Are deficiencies communicated to those parties responsible for taking corrective action, senior management and the board of directors (or audit committee)?	☐	☐	
17.4	Are the results of the internal audit activities reported to the following, as appropriate (and in accordance with the relevant reporting requirements): a) Senior management b) Board of directors or audit committee c) Independent auditors	☐	☐	
17.5	Are policies and procedures in place to ensure deficiencies are communicated externally, as required?	☐	☐	
17.6	Does management take adequate and timely actions to correct deficiencies reported by the internal audit function and by other monitoring activities?	☐	☐	
17.7	Does management respond timely and appropriately to the findings and recommendations of the independent auditors regarding internal control and policies and procedures of the organization?	☐	☐	
17.8	Is there a process in place to track unremediated control deficiencies and a protocol to escalate them to higher levels of management if necessary?	☐	☐	
Other		☐	☐	

Appendix B – Example Documentation Template

This template is provided as an example that organizations can consider when linking their existing internal control structure to the 17 principles and to identify any gaps.

Control environment: The set of standards, processes, and structures that provide the basis for carrying out internal control across the organization
Principle 1: The organization demonstrates a commitment to integrity and ethical values.
Points of Focus: 1. Sets the tone at the top – The board of directors and management at all levels of the entity demonstrate through their directives, actions and behaviors the importance of integrity and ethical values to support the functioning of the system of internal control. 2. Establishes standards of conduct – The expectations of the board of directors and senior management concerning the integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the organization and by outsourced providers and business partners 3. 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 4. Addresses deviations in a timely manner – Deviations from the entity's expected standards of conduct are identified and remedied in a timely and consistent manner.

Control reference	Description of control or activity	Related point of focus

Documents reviewed:		
Gaps identified, if any:		
When were the controls last performed?		
When were the controls last reviewed?		
Controls operating effectively?		
Were deficiencies identified (yes/no)?		

No.	Description of deficiency	Control reference

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

SCORE no. EE0946

This and many of the publications produced by our US Professional Practice Group, are available free on AccountingLink at www.ey.com/us/accountinglink.