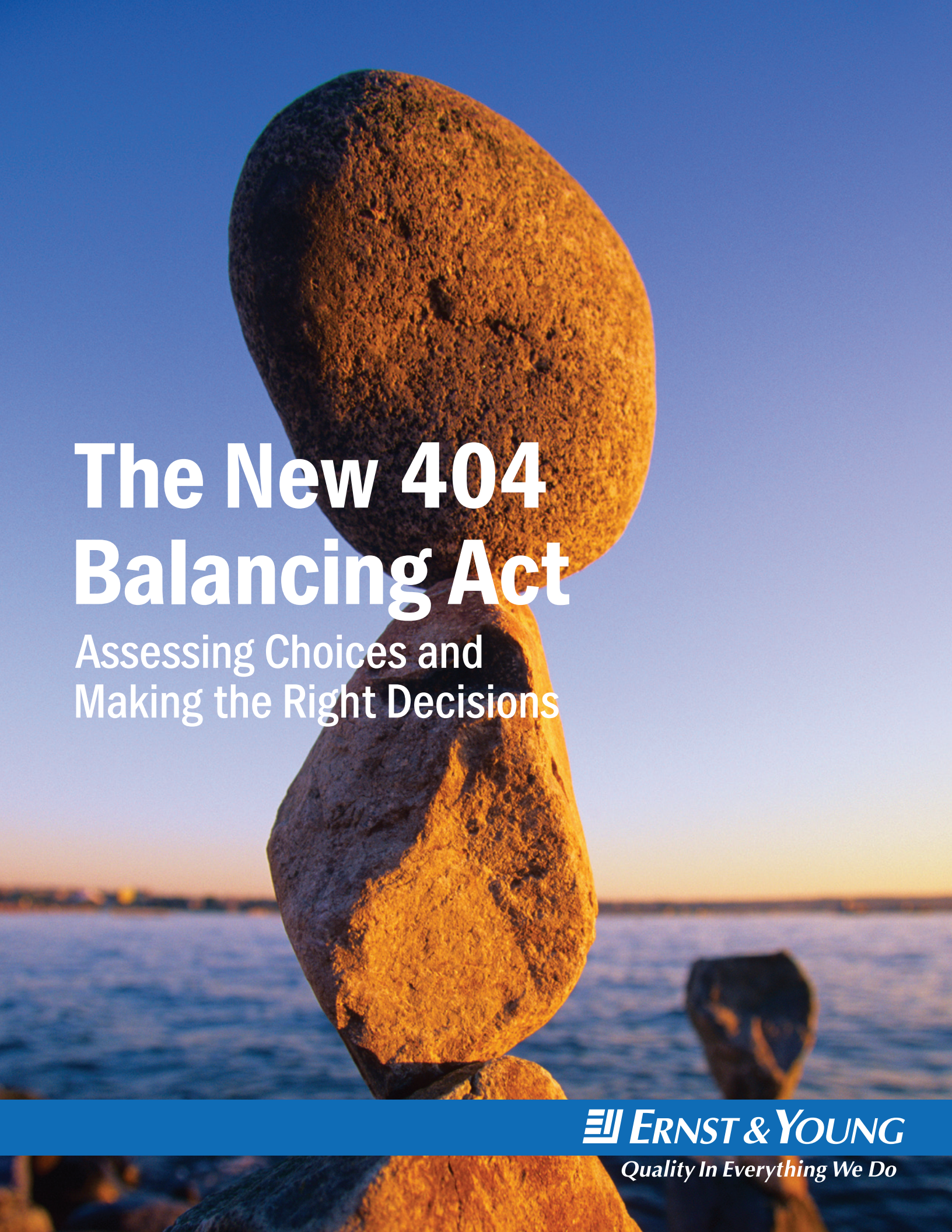


The New 404 Balancing Act

Assessing Choices and Making the Right Decisions

ERNST & YOUNG

Quality In Everything We Do

Highlights of SEC Management Guidance

On May 23, 2007, the Securities and Exchange Commission (SEC) unanimously adopted the following:

- Interpretive guidance for management's planning and conduct of its annual assessment of internal control over financial reporting required by Section 404 of *The Sarbanes-Oxley Act of 2002* (the "SEC Management Guidance"), and
- Certain rule amendments that:
  - More clearly convey that in fulfilling its reporting requirement pursuant to Section 404(b) of *The Sarbanes-Oxley Act of 2002* the auditor is not evaluating management's assessment process but is opining directly on the effectiveness of internal control over financial reporting (a single opinion on the effectiveness of internal control), and
  - Make it clear that a company choosing to perform an evaluation of internal control over financial reporting in accordance with the interpretive guidance would satisfy the annual evaluation required by SEC rules.

The SEC Management Guidance is based on two principles:

- Management should evaluate the design and operating effectiveness of controls to determine whether they adequately address the risk that a material misstatement would not be prevented or detected in a timely manner, and
- Management's evaluation of the evidence about the operation of its controls should be based on its assessment of risk.

While COSO and other recognized internal control frameworks provide the criteria for effective internal control, the SEC Management Guidance addresses how to conduct an assessment of internal control over financial reporting and is organized around the following topics:

- ***Identifying Financial Reporting Risks,***
- ***Identifying Controls that Sufficiently Address Identified Financial Reporting Risks,***
- ***Evaluating Evidence that Identified Controls are Operating Effectively, and***
- ***Reporting the Results of Management's Assessment.***

The SEC Management Guidance's discussion of each of the above evaluation elements provides companies with opportunities to challenge and improve upon their existing assessment process. For more detailed information regarding the SEC Interpretive Guidance, refer to "Internal Control Reporting Provisions" (Release Nos. 33-8810, 34-55929, FR-77; File No. S7-24-06; June 20, 2007) available through www.sec.gov.

Dear Clients and Friends

Has the 404 landscape changed?

Extensive testing of internal control systems—some would say *over*-testing—has become a fact of life for management since the inception of *The Sarbanes-Oxley Act of 2002*. But the new SEC interpretive guidance on achieving the objectives of Section 404 underscores management's flexibility in meeting 404 program requirements.

The SEC Management Guidance confirms what many have believed all along—that management can follow a top-down, risk-based approach when assessing internal controls. This is a very positive development because, as everyone with finance and operational responsibilities knows, all risks are not equal. Management's effort is best tailored to areas of greatest risk to reliable financial reporting.

This clarified guidance confirms opportunities to:

- Design a 404 process that is fully consistent with management's overall risk mitigation efforts.
- Incorporate effective entity-level controls to improve overall 404 program efficiency and effectiveness.
- Improve coordination among all 404 program participants.

In short, management can begin to think about improving processes and managing costs more effectively, without sacrificing the quality of the 404 program effort.

The SEC Management Guidance provides a roadmap to designing a more efficient 404 process, but one without detailed driving directions. Management should also look elsewhere for ways to improve its approach to 404. To lessons learned over the past three years of implementation, for instance. To leading organizations that are already adopting a top-down, risk-based approach. And, of course, to Ernst & Young.

We hope you find this publication, the first in a series, eye-opening and well worth your reading time. We encourage you to use the program self-assessment tool and the outline of a transformation approach, reprinted in the appendices, to take a fresh look at your 404 program. And then we invite you to contact Ernst & Young to explore ways we can work together to achieve the new 404 balancing act.

Sincerely,

Ernst & Young LLP

Contents

The New 404 Balancing Act

It's no secret that implementing the provisions of Section 404 of *The Sarbanes-Oxley Act of 2002* (Section 404) has been expensive and resource-consuming for publicly listed companies in the U.S. Most companies have by now acclimated themselves to the almost year-round internal controls (IC) assessment process, and extensive IC testing has become a fact of life for management. Companies are looking for ways to improve efficiencies while also extracting greater value from their 404 programs.

In response to the heightened regulatory environment of the past three years, the majority of companies responded to Section 404 by implementing comprehensive Section 404 programs that potentially go beyond what is needed to provide management with reasonable assurance that the company's system of internal control over financial reporting is effective. Long-awaited SEC Management Guidance, however, encourages companies to sharpen their focus on areas of greatest financial reporting risk. Management should not underestimate the importance of this opportunity and the chance to re-evaluate its 404-related activities.

Time to Take a Breath

The velocity of change associated with 404 implementation and the enormity of the task, coupled with the uncertainty surrounding the regulations, left little time to evaluate and improve the 404 game plan. Many companies have not had a chance to reflect on the 404-related decisions they initially made during the race to implement IC reporting, nor have they benefited from flexible, principles-based SEC Management Guidance—until now. The SEC Management Guidance encourages management to follow a "top-down, risk-based" approach in assessing and reporting on internal controls. This means that companies can challenge the degree to which risk assessment drives their scoping activities and begin at the top—at the level of the financial statements. Management's risk-based scoping, starting at the top, recognizes that all accounts and related risks are not equal, and that management's effort is best tailored to focus more attention on areas of greatest risk to reliable financial reporting. We believe most companies can utilize the SEC Management Guidance to reconsider the IC assessment process itself, with a view to streamlining efforts and reducing cost. Now might be a good time for management to take a breath, step back, and reconsider.

Streamlining the IC assessment and reporting process, however, will require thoughtful expertise and insight. The SEC Management Guidance sets out basic principles—but does not provide detailed instructions for this purpose. Management should also look elsewhere for ideas and models on which to base their process improvement initiatives.

Key Terms	
Entity-Level Controls (ELCs)	Broad-based, company-wide controls that have a pervasive effect across the organization. The term "company-level" is also commonly used to describe these controls.
Internal Control Over Financial Reporting (ICFR)	A process designed by management that is intended to provide reasonable assurance regarding the reliability of external financial reporting.
Program Management Office (PMO)	The project team assigned the responsibility for defining and communicating the overall 404 strategy for the company, managing the program implementation, and reporting progress to key stakeholders.
Top-Down, Risk-Based Approach	The approach to conducting an ICFR assessment that identifies the risks related to reliable financial reporting, the combination of controls that effectively and efficiently addresses those risks, and evaluates the evidence necessary to conclude on the effectiveness of such controls. The approach rests on the premise that not all risks are equal, and management's effort should be tailored according to the nature (likelihood and magnitude) of the identified level of risk.
Transformation	The evaluation of a company's existing 404 program in considering the SEC Management Guidance and lessons learned. Successful 404 transformation results in a sustainable top-down, risk-based approach that is effective, efficient, and consistent with stakeholder expectations relative to internal control assessment.
SEC Management Guidance	The SEC's interpretive guidance for management on conducting an assessment of internal control over financial reporting under Section 404 of *The Sarbanes-Oxley Act of 2002*.
404 Program	The company's overall governance and associated activities to implement the internal control reporting requirements of *The Sarbanes-Oxley Act of 2002*. A 404 program encompasses governance, project management, people, methodology, and technology.

Learn from Experience

Even great companies can learn from other great companies. Chief among lessons learned in the first years of implementation are these:

- Companies that leverage a top-down, risk-based approach, which includes relying on effective entity-level controls, have significantly more efficient 404 programs than those that do not.
- Companies that leverage a top-down, risk-based approach can redirect their efficiencies (i.e., cost savings, resources) to other critical areas of the business.
- Companies that understand the components of their total 404 expenditures are best positioned to manage overall program costs.

The SEC Management Guidance encourages companies to manage their 404 costs—and their risk mitigation strategy—more proactively, through top-down planning. The guidance also creates opportunities to:

- Further understand and address significant financial reporting risks.
- Challenge the design and implementation of entity-level controls, including monitoring controls.
- Improve coordination among all program participants.
- Design a sustainable 404 process that is fully integrated and consistent with management's overall internal control structure.

In short, the SEC Management Guidance is an opportunity to significantly enhance the efficacy and efficiency of a company's Section 404 program.

Develop a Point of View

The SEC expects that each organization's approach to implementing IC reporting will correspond to its unique financial reporting risks and related controls. The SEC Management Guidance is designed to focus more of management's attention on the areas of greatest risk, and reducing, but not necessarily eliminating, attention on other areas of risk to reliable financial reporting. The SEC Management Guidance further encourages management to use judgment to determine the method of evaluation most appropriate for the company and, therefore, accommodates a range of acceptable assessment methods. The guidance ultimately removes the uncertainty around how much flexibility management has in designing assessment programs that meet 404 program requirements.

Thus, while the SEC Management Guidance provides direction, it does not mandate particular assessment methods or create "bright lines" around key considerations. This flexibility invites companies to benefit from lessons learned during the first years of 404 implementation and the experiences of others. Management's judgment is still expected to yield an effective, top-down, risk-based approach to its Section 404 assessment process. While some companies have begun to adopt a top-down approach to risk assessment, few have fully applied this approach to identifying controls to address these risks and even fewer have fully tailored the nature and extent of evidence gathered to conclude that controls are effective.

Assess Choices and Make the Right Decisions

To date, companies have addressed Section 404 through a wide variety of approaches and organizational models. Some companies rely heavily on process and control owners to identify, assess, and evaluate their own key controls, while others have relied exclusively on separate evaluations conducted by testing authorities, such as newly established control functions or expanded internal audit functions.

Many companies that have sought to implement a top-down, risk-based approach have found that it was harder than originally anticipated and as a result suffered slower than expected progress. Others acknowledge that their assessments are more about coverage than risk, and thus are more arduous and resource-consuming than they would prefer.

Clearly, methods of applying the SEC Management Guidance are as varied and unique as each company subject to the Section 404 requirements.

Choices Mean Change

Whatever path a company takes relative to implementation of the SEC Management Guidance (aside from continuing the expensive status quo), there will be important change management considerations. Transforming the 404 program will certainly affect program stakeholders—from the board of directors and audit committee to top management, auditors, investors, and analysts—and do so differently based on the organization's unique business, location, structure, market, and competitive situation. For example, any substantive changes are likely to affect the external audit reliance strategy and should be made with this potential effect in mind. Importantly, before making significant changes, it is critical that management consider the perspectives of key stakeholders to determine that important risk and cost factors are appropriately understood and acted upon.

Each organization will need to define goals relative to its 404 program requirements, coverage, cost, and the potential effect on the external auditor's strategy. The flexibility offered in the guidance will allow management to challenge the status quo and build a sustainable, cost-effective, and valuable internal controls assessment for the organization. Since 2002, some organizations have focused on their 404 program at nearly any cost, which has led in some cases to gross inefficiencies far out of balance with any risk mitigation benefits. It is clear that the SEC Management Guidance affords management the opportunity to re-balance this compliance-cost-risk equation and allocate more resources to the areas of higher risk.

There is a way to get from here to there. Let's explore the choices available that can lead to making the right decisions. We'll start by exploring different opportunities available through a discussion on the top-down, risk-based approach and conclude with next steps to consider.

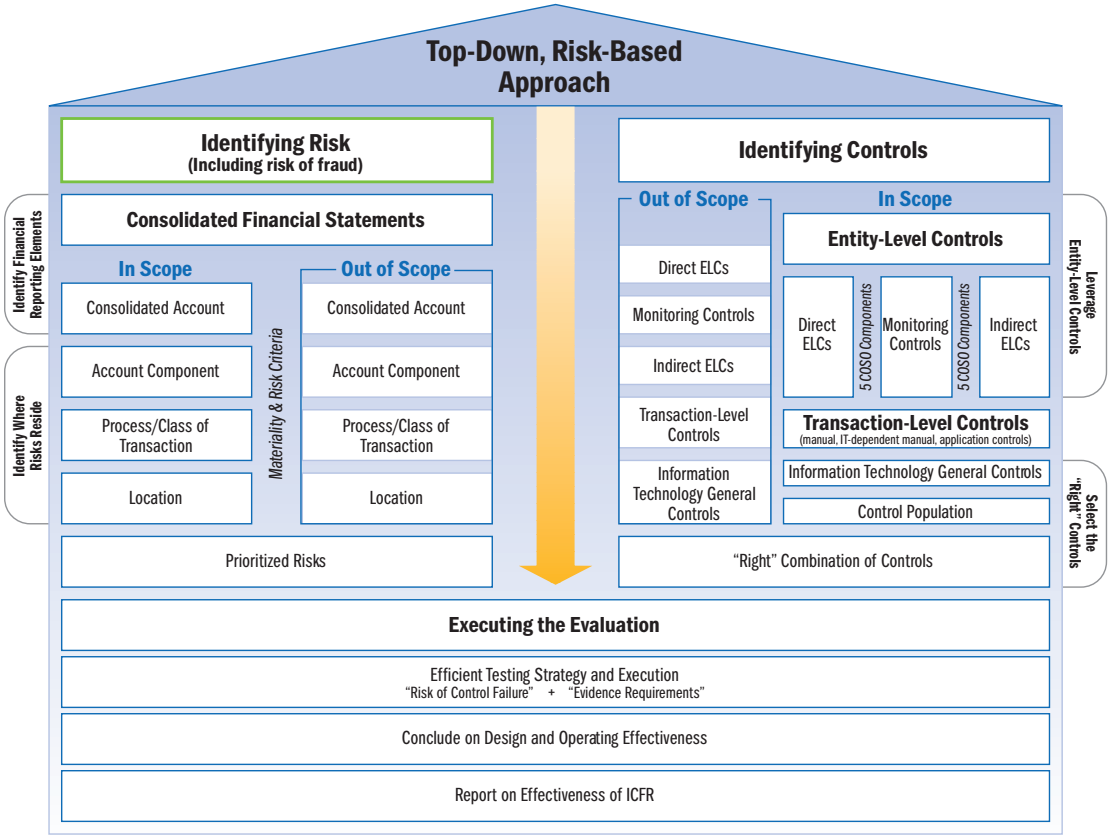
Making Top-Down, Risk-Based Choices

Management's assessment process determines whether there is a reasonable possibility that the organization's internal control over financial reporting (ICFR) will fail to prevent or detect, in a timely manner, a material misstatement in the financial statements and disclosures. One important lesson we have learned over the years is that this goal can be achieved more efficiently with a top-down, risk-based approach. The top-down, risk-based approach represents a thought process—a management perspective—that focuses on the organization as a whole and drives allocation of more resources to the areas of highest risks to reliable financial reporting and effective ICFR. It is not driven by a checklist mindset.

Another key lesson has to do with how this top-down, risk-based approach is applied. Leading companies consider not only their financial reporting risks, but also the risks related to their controls. When performing their top-down risk assessment, leading companies identify the combination of controls (entity-level, transaction-level) that best supports an effective and efficient assessment, and determine early-on the level of evidence required to conclude such controls are effective. Throughout the entire assessment process, management must exercise risk-based judgments to align the nature, timing, and extent of its evaluation procedures with those areas that pose the greatest risk to reliable financial reporting.

All of these factors and considerations can make implementing a top-down, risk-based process a complex, yet rewarding, task for companies. To help explain the top-down, risk-based approach, we have created a model with three main activities: risk identification, controls identification, and execution of the evaluation. These activities, when undertaken together, provide management with a path to achieving reasonable assurance regarding the reliability of its financial reporting. The entire model rests on a foundation of prioritized areas of risk and the "right" combination of ICFR.

Applying a Top-Down, Risk-Based Approach



"The Model"

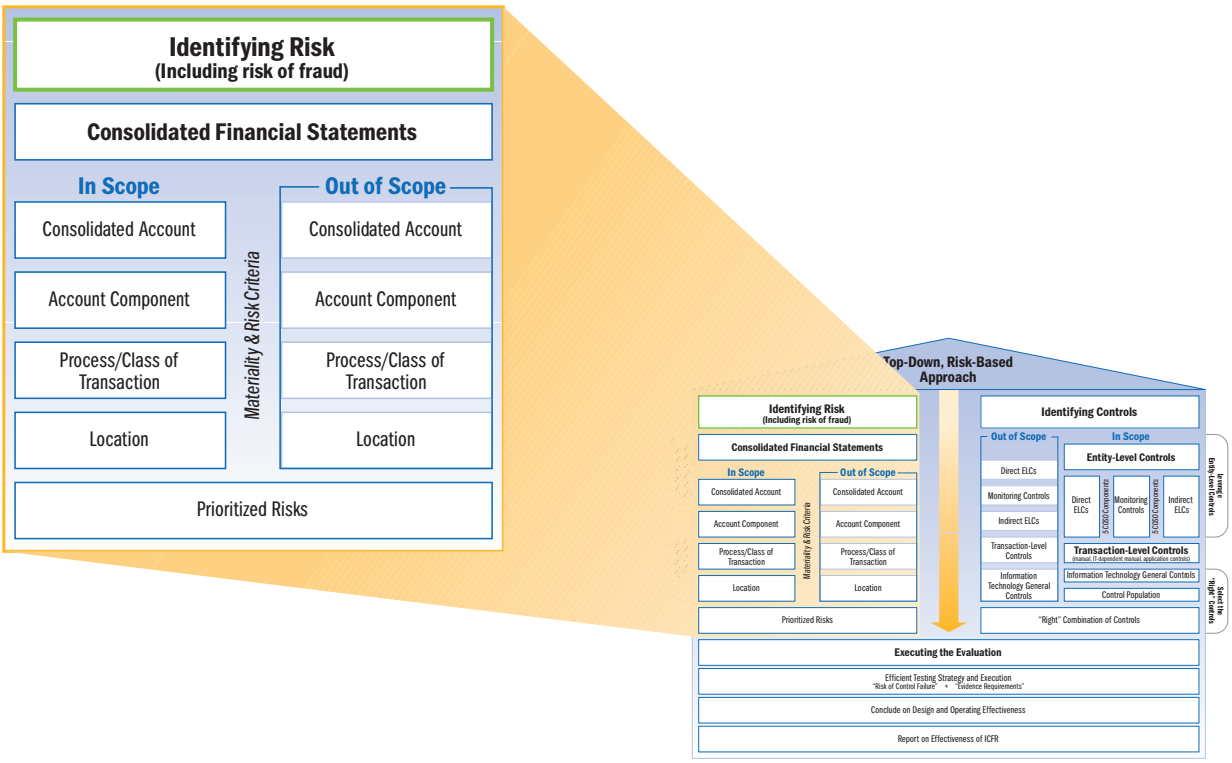
The risk assessment activities involve identifying and assessing material financial reporting risks. Assessment of financial reporting risks begins with management's judgment of what is material to the consolidated financial statements followed by a thorough risk assessment that considers the characteristics of individual financial reporting elements and the likely sources of misstatement within the significant processes that operate across a company's locations. Among leading organizations, management prioritizes material financial reporting risks using customized risk assessment criteria. These customized criteria allow management to prioritize and document risks and facilitate consistent application across the company. The importance of management's judgment and knowledge of the business cannot be emphasized enough in determining and prioritizing risk.

Similarly, as we have learned in working with leading organizations, the controls identification activity defines the "right" combination of controls to sufficiently address the identified financial reporting risks. Just as with risk assessment procedures, the new SEC Management Guidance encourages management to apply a top-down approach to identifying the controls that address risks. This includes the identification of indirect ELCs, which are pervasive in nature and help to establish the control environment; and direct ELCs, which, if effective, sufficiently precise, and linked to specific accounts and assertions, can be leveraged by management to address identified financial reporting risks, individually or in combination with transaction-level controls (including application controls).

Once the "right" combination of controls is selected, the model is supported by a well-designed, efficiently executed testing strategy for identified controls that considers the level of evidence required to support management's assessment. Leading companies vary the level of evidence gathered based on their assessment of the risk characteristics of individual financial reporting elements and the related identified controls (collectively "ICFR risk").

It is worth mentioning that one of the critical success factors in implementing a top-down, risk-based approach is the availability of information and data pertaining to financial reporting elements, processes, and locations. Organizations that have a clear understanding of how their financial reporting elements are supported by relevant information systems, including how significant processes exist across multiple locations, are generally better positioned to successfully implement the SEC Management Guidance. While some organizations may be able to leverage their current understanding and documentation of financial reporting elements, information systems, processes, and locations, many organizations can improve the efficiency and effectiveness of their application of the top-down, risk-based approach by increasing their visibility into the structure and data supporting the consolidated financial statements. While not always an easy task, without visibility into this structure and data, a company's ability to implement a top-down, risk-based approach may be significantly impaired.

Identifying Financial Reporting Risks



Risk has been high on boards' and management's agendas since well before *The Sarbanes-Oxley Act of 2002* became law. The capital markets are placing more emphasis on risk and risk management activities employed by organizations to ensure their objectives are met—be it financial, operational, compliance-oriented, or strategic.

In Ernst & Young's view, risk assessment is a continuous element in planning the overall assessment and is the cornerstone to an efficient and effective 404 program. This is why Ernst & Young encourages organizations to build their own model, that is, to transition or transform their 404 programs with top-down, risk-based planning activities that can deliver effective compliance to 404 program requirements with greater efficiency. A well-thought-out transition or transformation approach will be the key to reaping the many benefits this model implies. (We outline a transformation approach in Appendix B.)

Management should first consider the generally accepted accounting principles (GAAP) that apply to its organization and the related risks to fair presentation of the financial statements. The SEC Management Guidance advises management to use its knowledge and understanding of the business, its organization, operations, and processes to consider the sources and potential likelihood of misstatement in financial reporting and identifies those sources that could result in a material misstatement to the financial statements ("financial reporting risks"). Internal and external risk factors impacting the business, including the nature and extent of any changes in those risks, may give rise to financial reporting risks.

Financial reporting risks may also arise from the initiation, authorization, processing, and recording of transactions and other adjustments that are reflected in financial reporting elements. The SEC Management Guidance states management's evaluation of financial reporting risks also should consider the vulnerability of the company to fraudulent activity (for example, fraudulent financial reporting, misappropriation of assets and corruption) and whether any of those exposures could result in a material misstatement of the financial statements.

The following discussions outline some of the areas within risk assessment activities where management may challenge customary thinking and identify further opportunities to make the 404 program more efficient.

Efficiencies from Materiality Decisions

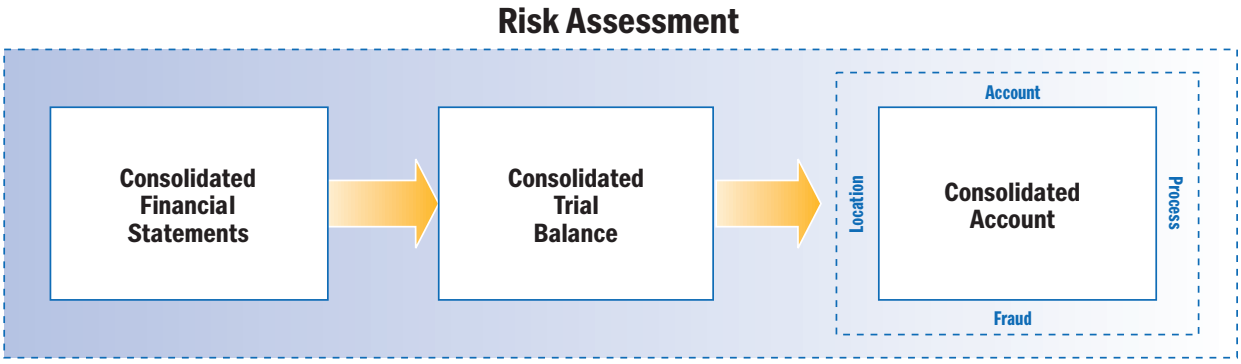
Materiality thresholds are an important consideration for management's assessment. While overall materiality is, in large part, a quantitative consideration based on key financial measures (e.g., income, revenues), it also is important to consider inherent risks of misstatement, the expectations of key stakeholders, and other qualitative factors. Management should revisit levels of materiality used to identify in-scope financial reporting elements and financial reporting risks to determine that materiality thresholds reflect the current size and complexity of the company and relevant qualitative factors.

Management should also revisit materiality levels assigned to the company's various business units looking for opportunities to more efficiently address the risks of aggregated financial misstatements.

Key Insight	• Challenge whether overall and business unit-level materiality thresholds appropriately reflect both quantitative and qualitative factors.
Question to Consider	• To what extent have you revisited materiality factors that may have changed?

Efficiencies from Financial Reporting Elements

SEC Management Guidance refers to "Financial Reporting Elements" (FR elements) as the financial statement accounts and disclosures that make up the organization's consolidated financial statements. In leading organizations, management breaks down consolidated financial statement line items and footnote disclosures into individual FR elements to determine those that are material. In adopting this approach, management uses its judgment and knowledge of the business to carefully assess risks in these FR elements. This exercise is very important as individual consolidated accounts can be made up of many components, each with different levels of materiality and risk.



This experience leads us to conclude that management should exercise judgment and leverage its knowledge of the business to determine risks specific to the organization. For instance, an account may contain one or more characteristics of risk yet still be determined to be low risk due to the low probability of a material misstatement associated with this account. On the other hand, there are some accounts that although they may be of low monetary value compared to other accounts, should be included in scope due to their higher risk of material misstatement based on qualitative factors.

The SEC Management Guidance sharpens the focus on fraud as part of the top-down, risk-based assessment. The likelihood of fraud occurring generally increases when one or more fraud risks are present, particularly in an environment where significant pressure exists to meet financial or operational targets. As a result, understanding internal control at the entity level—especially the tone-setting level—becomes increasingly important in helping management identify and analyze potential risks of fraud.

There are three conditions usually present when people commit financial fraud or misappropriate assets:

- Incentives or pressures to perpetrate fraud to achieve desired financial results.
- Opportunities to carry out fraud without being detected (e.g., controls are deficient or missing).
- Personnel who are able to justify or rationalize their fraudulent activities.

Management should consider the fraud risk factors at the account, assertion, process, and location levels as part of its approach to evaluating ICFR. Often, fraud controls are identical to those controls identified to detect or prevent misstatements in the financial statements.

Key Insights	• Drill down to components of accounts that are subject to differing risks and processing to determine what is in scope. • Daily involvement may provide you with adequate knowledge to identify financial reporting risks and mitigating controls. • Apply a top-down risk-based approach to identifying fraud risks.
Questions to Consider	• How did your approach to classifying risk affect your overall effort? • To what extent have you tested components of accounts in various locations that are subject to the same processing and risks? • To what extent has your risk assessment taken fraud into consideration?

Efficiencies in Financial Reporting Risk Assessment Criteria

Once risks are identified that will be "in scope," management should prioritize these risks. This prioritization will be important for future activities such as facilitating better risk-based control identification and developing testing strategies. Best practice indicates that once financial reporting elements and related assertions have been identified, management should develop customized risk assessment criteria, including the risk of fraud. These risk assessment criteria would consider the impact and likelihood of potential misstatement as well as aid in prioritization of risk related to these elements. Risk rating and prioritization are *judgmental processes* and therefore highly dependent on the experiences of participants involved in the process. Validating risk criteria and prioritization outcome is crucial.

Key Insights	• Do not scope out material accounts assessed as low risk. Rather, tailor the nature, timing, and extent of testing so that the amount of evidence gathered is commensurate with the identified risk. • Risk assessment for accounts below materiality should incorporate the risk of understatement.
Question to Consider	• Have you considered both risk and materiality in determining scoping of financial reporting elements?

Efficiencies in Considering Significant Processes and Locations

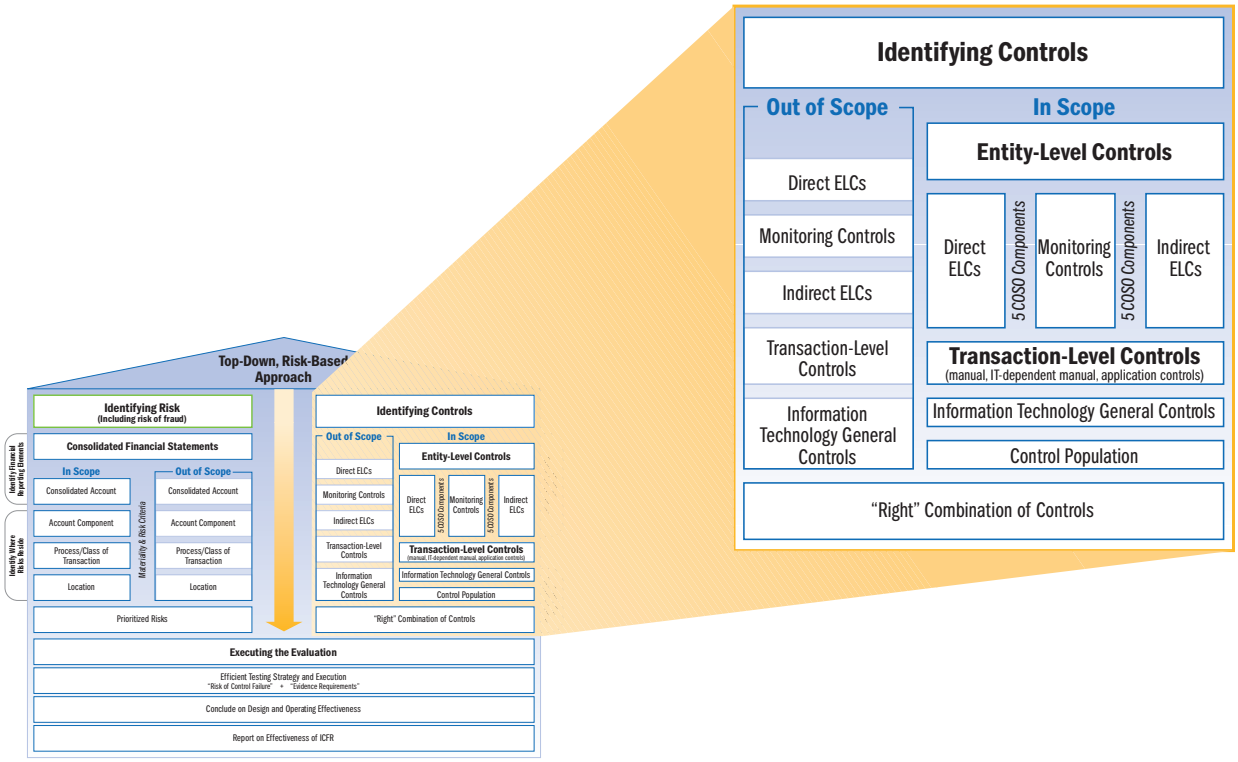
To understand risks within financial reporting elements, management is encouraged to identify the major classes of transactions affecting those financial reporting elements and the related significant processes. By "significant processes" and "classes of transactions" we mean those that materially affect the FR elements. Different types of transactions have varying levels of risk and likelihood of errors. For example, classes of transactions might be routine and involve frequently recurring financial data. Other classes of transactions might be non-routine or involve estimation or numerous judgments and assumptions and therefore represent higher risk. The classification of each process and major class of transaction by type aids management in identifying and prioritizing the specific risks affecting the various financial reporting elements.

Where classes of transactions are similar across multiple locations there may be opportunities to evaluate the risks and identify and test controls on an aggregated basis similar to that of a business with a single location or business unit. The opportunity to do so increases where processing is centralized or where processes and controls have been centrally designed and are subject to common ELCs. However, where risks vary across locations or the classes of transactions are subject to unique processing and control environments, it is more likely that controls at each significant location will need to be evaluated individually. Common systems and centralized processing can serve to reduce risks across an organization; however, minor control breakdowns can have pervasive effects and thus present a different form of risk.

Management should understand its financial reporting elements sufficiently to identify financial reporting risks, which often is most efficiently and effectively done by looking at the way that major classes of transactions flow through the significant processes. In doing so management can determine the locations where processes and risks reside and scope processes across various locations based on assessed level of risk and materiality.

Key Insights	• Determine financial reporting risks before scoping significant locations. • Focus on how processes and classes of transactions operate across a company's locations. • Consider how locations contribute to key financial reporting risks.
Questions to Consider	• What drove your scoping in previous years? Locations? Risks? • Did you focus on all processes for in-scope locations or apply risk-based considerations?

Identifying Internal Controls over Financial Reporting



The controls side of the model has to do with the "right" combination of controls that adequately addresses the company's financial reporting risks. We emphasize the word "right" because management has the flexibility, and the SEC Management Guidance supports this notion, to consider efficiency with which controls can be evaluated when determining which combination of controls should be selected for testing as part of its assessment.

Among leading organizations, management applies a top-down, risk-based approach to identifying controls that address financial reporting risks by first considering entity-level controls (ELCs) and then transaction-level controls (TLCs). The premise behind this approach is that, in general, ELCs that are pervasive in nature may be more efficient and effective in addressing risk *across the organization*. The SEC Management Guidance highlights three types of ELCs:

- Controls that are indirectly related to a financial reporting element and ordinarily are not, by themselves, effective at preventing or detecting material misstatements.
- Controls that identify possible breakdowns among lower-level controls, though not in a manner that would, by themselves, sufficiently address the risk that material misstatements in financial reporting will be timely prevented or detected.
- Controls that operate directly at the process, transaction, or application level and are designed to timely prevent or detect material misstatements in one or more financial reporting elements.

Most ELCs are not designed to have the necessary precision and direct relationship to accounts and assertions to, by themselves, address the risk. In most cases it will be necessary to identify a combination of ELCs and TLCs to gather sufficient evidence that controls adequately address a particular risk. But in general, as ELCs increase in precision and more directly relate to specific financial reporting elements and assertions, the more reliance management may be able to place on them. This may result in management needing less evidence to support the operating effectiveness of certain TLCs that operate in combination with ELCs to address risks related to specific financial reporting elements and assertions.

The level of risk priority frequently affects the selection of the "right" combination of controls. For example, management's ability to rely on ELCs to address risks for more complex financial reporting elements may diminish as the risk of control failure increases with the increased complexity of the reporting activity. ELCs may have little impact on the accounting and reliable financial reporting for highly complex transactions requiring significant skill and knowledge. Management must consider these relationships and complexities when selecting combinations of controls.

Key Insights	• Look at the control population and select the "right" combination of controls that most efficiently and effectively addresses identified financial reporting risks. • Leading companies have recognized two significant benefits to identifying and linking ELCs to specific risks. First, when direct ELCs are linked, a lesser number of TLCs are generally necessary to address the identified risks. Second, the presence of direct ELCs as part of a combination of controls to address identified risks reduces the overall risk profile of other associated controls, thus reducing the level of evidence necessary to conclude such controls are operating effectively.
Question to Consider	• What drove selection of the combination of controls in your organization?

Leveraging ELCs

Evaluation of a system of internal control using a suitable control framework necessarily must include those policies, procedures, and activities that address the elements that the applicable control framework describes as necessary for an internal control system to be effective. For example, COSO describes five components essential to a system of internal control. Management's evaluation process must include not only controls over particular areas of financial reporting risk, but also the entity-wide and other pervasive elements of internal control defined by its selected control framework. Therefore, an effective system of internal control includes a balance of ELCs and TLCs that work in combination. For most areas of financial reporting risk, both will need to be evaluated and tested to conclude on the overall effectiveness of internal control over financial reporting because management generally designs its system of internal control to rely on both types of controls working together to address risks.

Key Insights	• More direct corroborative evidence is required as the risk associated with an account increases. • ELCs such as monitoring controls could be leveraged to reduce testing in low risk areas.
Questions to Consider	• Have you leveraged ELCs in reducing your testing? • Have you considered efficiencies when selecting the combination of ELCs and TLCs?

Early in the history of Section 404 implementation, many companies executed their evaluation of ELCs as a stand-alone process, without linking them to the financial reporting risks. Moreover, ELCs have long been associated only with the control environment, and often have not been considered in relation to other internal control components: risk assessment, control activities, information and communication, and monitoring. As a result, ELCs have been under-leveraged to reduce the overall testing effort.

Furthermore, in the past, ELCs were often addressed late in the assessment process. Many organizations instead focused first on their inventory of transaction-level controls believed necessary to meet the SOX requirements. Consequently, a significant portion of management's time and effort went to documenting and remediating the deficiencies identified during the testing of the transaction-level controls. Leading organizations have developed a thorough understanding of ELCs, how they help to address specific risks and the value their identification and linkage can bring to a top-down, risk-based approach. They utilize these controls, where appropriate, as part of the "right" combination of controls to address identified risks. As a result, these companies test fewer transaction-level controls.

Effective ELCs directly impact the efficiency of the 404 program. When ELCs are operating effectively, management enjoys a higher level of confidence that the transaction-level controls identified will continue to function effectively over time. This understanding positively impacts the risk assessment and the nature, timing, and extent of control testing. Understanding ELCs early in the evaluation process allows leading organizations to leverage these controls throughout the process. Effective ELCs also play a prominent role in an effective control environment and provide for a more effective risk assessment.

Key Insights	• Historically, ELCs were evaluated and tested towards the end of the assessment process, and focused primarily on those controls within the control environment, reducing their ability to be leveraged in the top-down, risk-based approach. • Deficient ELCs were a key contributor to reported material weaknesses.

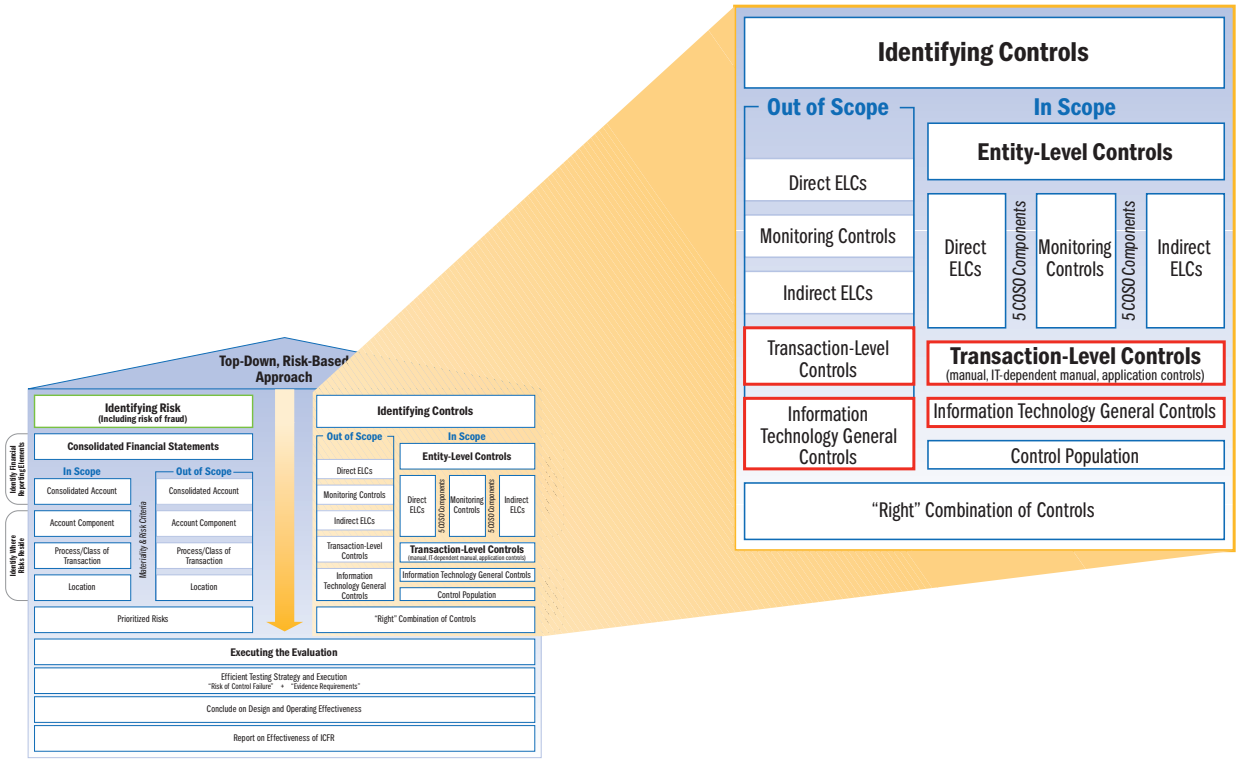
The SEC Management Guidance has brought ELCs to the front of the 404 process. It should refocus management's attention on the efficiencies that can be derived from effective ELCs. Thus, ELCs should be considered early in the process and appropriately leveraged as part of the top-down, risk-based approach. Adopting such an approach will affect how management evaluates the other aspects of internal control over financial reporting and will also provide the ability to remediate any ELCs that are not functioning as designed.

In a top-down, risk-based approach, the identification and evaluation of effective ELCs can help management increase the efficiency of its testing in lower risk areas and redirect resources towards higher risk accounts. This helps increase both the effectiveness and efficiency of management's Section 404 program.

To summarize the key issues regarding ELCs:

- ELCs are associated with each of the five COSO components (control environment, risk assessment, control activities, information and communication, and monitoring).
- Management should consider the level of risk, the nature of the control, and the objectivity of the person performing the control in determining the persuasiveness of evidence that can be obtained from ELCs. (For example, as the risk level increases, it is more likely that it will be necessary to gather more evidence through testing TLCs since the evidence gathered from testing ELCs frequently will not be sufficient to conclude that the FR risks have been addressed. On the other hand, as the risk level decreases, companies may find it more efficient to look first to direct ELCs, rather than solely relying on TLCs.)

Leveraging Information Technology Controls



IT plays a vital role in an organization's system of internal control. As shown in the above diagram, IT controls consist of application controls, IT-dependent manual controls, and IT general controls (ITGCs). ITGCs include the controls over the IT environment, computer operations, access to programs and data, program development, and program change. ITGCs support the functioning of application controls and IT-dependent manual controls. All categories of IT controls are needed to ensure complete and accurate information processing.

ITGCs and Material Weaknesses. Information technology impacts organizations' financial reporting processes, and, by extension, their 404 programs. In an analysis of Section 404 material weaknesses, Ernst & Young found that a quarter of survey participants cited IT as at least a contributing factor. Four out of five organizations cited access to programs and data files as an issue and one in three cited controls over changes to programs as an issue. Additionally, many companies concluded that they tested too many IT controls without a corresponding benefit to addressing financial reporting risks. Over-scoping IT led to excessive costs in the early years.

Top-Down, Risk-Based Approach to Testing IT Controls

A top-down, risk-based approach to testing IT controls starts with first determining those applications and associated automated or IT-dependent manual controls that are important to the assessment of IC, and then determining the ITGCs that are relevant to those applications and associated automated or IT-dependent manual controls. Thus, if it is determined that no automated or IT-dependent manual controls are in scope for a given account or process, management need not test the related ITGCs. Because the assessment of ITGCs was often handled as a separate evaluation process, this approach was not always considered in the early years of 404, which contributed to over-scoping and over-testing of ITGCs.

This approach provides flexibility in designing a strategy for evaluating the effectiveness of transaction-level controls that depend on IT for their proper functioning and will help avoid unnecessary testing of controls that are not important to management's assessment. We discussed earlier establishing the "right" combination of controls to address a related risk. In areas where automated controls are to be relied on, or controls depend on electronic evidence, management should consider the effect of the related ITGCs and challenge the level of ITGC scoping in areas where such automated controls are not identified, or represent a smaller number of the combination of controls that have been identified. Further, it may be possible to vary the number and type of ITGCs identified commensurate with the number, type, and level of risk related to the underlying automated controls the ITGCs are designed to support. Management should consider both the risks expressly associated with each ITGC it intends to address, and the nature, timing, and extent of testing to perform on those ITGCs.

Efficiency through scalability. The top-down, risk-based approach to identifying and testing IT controls supports scalability to smaller organizations. For example, smaller, less complex organizations that utilize packaged software may be able to reduce their testing of ITGCs. By using packaged software, management may not have to test controls over such processes as program changes and program development.

Efficiency through aggregated testing. In more complex organizations with numerous business locations, management may be able to aggregate ITGC testing so long as the ITGCs to be tested are similar across multiple applications, locations, or technical components (such as operating systems, database management systems, or applications). This means that management can rely on the testing of a single sample instead of multiple samples. Obviously, the more decentralized or dissimilar the technology and procedures of an organization's IT environment, the less likely ITGCs can be tested in this way.

Efficiency through "test-of-one" approaches. Effective ITGCs enable management to reduce testing of application-level controls. In certain cases, management may be able to rely on a "test of one" where the automated controls operate systematically and consistently and ITGCs provide reasonable assurance that an application control will function effectively over time. Thus, by limiting the testing sample, organizations can reduce related costs.

Efficiency through benchmarking. Another way to make the testing process more efficient is to benchmark certain tests of application controls from one testing period to another. Benchmarking acknowledges that a computer will continue to perform a given procedure (such as aging accounts receivable, three-way match, or an edit test) consistently until the program is altered. If it can be verified that a given program executing an automated control has not changed since it was last tested, or that the functioning of the application control has not changed, testing of the control may not need to be repeated. This "benchmarking period" might extend through year end and even into subsequent fiscal years.

Efficiency through continuous controls monitoring. Continuous controls monitoring (CCM) represents still another strategy for improving efficiency. This emerging technique, which monitors financial and operational controls at the entity and transaction levels, automates the monitoring process to help detect control failure and improve control performance. CCM focuses on application controls and segregation of duties, transactional data analysis, and ITGCs. Through the use of supporting tools, CCM can help reduce time spent gathering and analyzing data and testing procedures.

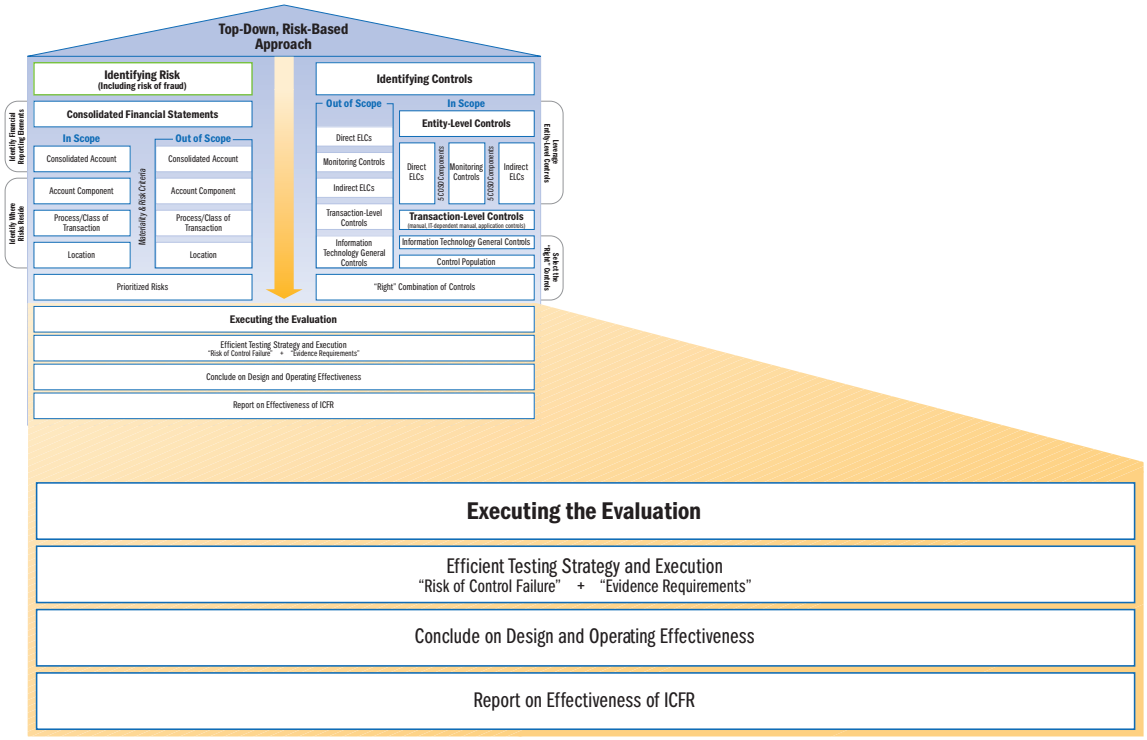
Key Insights	• Improving the mix of automated to manual controls contributes to efficiency. • You can increase the number of common ITGCs by standardizing, centralizing, and consolidating IT processes. • Consider using a benchmarking strategy.
Question to Consider	• Have you considered all options for leveraging IT to build more efficiencies in your 404 program?

Identifying Transaction-Level Controls

Transaction-level controls include manual controls, IT-dependent manual controls, application controls, and end-user computing controls. Management identifies only those transaction-level controls that address identified financial reporting risks and has the flexibility to not identify controls that are not important to achieving the objectives of ICFR. Furthermore, in identifying different controls or combinations of controls that address the identified risk, management has the flexibility to select controls for which evidence of operating effectiveness can be attained more efficiently. A top-down, risk-based approach thus allows management to focus resources on those controls that specifically address identified financial reporting risks.

Key Insights	• Select the most efficient transaction-level controls or combination of controls that effectively address financial reporting risks. • Selecting a "right" combination of controls is the most effective and efficient way to conduct a 404 assessment.
Questions to Consider	• Have you selected the most efficient transaction-level controls to test? • Are there ELCs which might displace some TLCs?

Evaluating ICFR



The SEC's interpretive guidance seeks to eliminate any uncertainty about management's flexibility to vary the nature, timing, and extent of testing based on the risk associated with the control and, therefore, the evidence actually needed for reasonable assurance that controls are operating effectively. Just as all financial reporting risks are not equal, the SEC Management Guidance expressly recognizes that the risks associated with individual controls also differ and that the persuasiveness of evidence that management needs to conclude controls are effective varies with the risk characteristics of the financial reporting elements to which the controls relate and the characteristics of the controls themselves. As the risk associated with a control increases, management may need to obtain more persuasive evidence in support of its assessment, and vice-versa.

Further, the SEC Management Guidance recognizes that management is in a fundamentally different position than the auditor. Management determines the basis for the evaluation of internal controls on the strength of its command of the business and operations—that is, management's perspective of the business environment, business operations, and their attendant risks to reliable financial reporting. Consequently, management is in the best position to determine the character and quality of evidence required to support its assessment about the operating effectiveness of internal control over financial reporting.

Management also should look at the nature of its ongoing monitoring activities and their ability to provide evidence about the continuing effectiveness of internal controls. After establishing that controls function effectively, management might use evidence from ongoing monitoring activities to determine that controls continue to function effectively. Ongoing monitoring activities can use either direct or indirect information from which management can draw conclusions about the effective functioning of controls. While either form of information can be effective, direct information ordinarily provides more persuasive evidence. More persuasive evidence may lengthen the period of time that can elapse before needing to obtain evidence of effective operation of controls from direct testing. This may be especially helpful in lower risk areas where less evidence may be needed to conclude that controls function effectively.

Determining the nature, timing, and extent of control testing is a matter of management judgment and varies according to the presence of a variety of factors, such as frequency of the operation of the control, persuasiveness of evidence produced by the control, the need to be satisfied that the control operated as intended, existence of a combination of controls that may reduce the level of evidence required of any individual control, and relative importance of errors that could result if the control was not functioning as intended.

The extent of testing also depends on other factors that relate to the likelihood that the control operated as intended, such as the competence of the person who performs the control, effectiveness of internal control at the entity level, changes in related processing procedures for classes of transactions, unexplained changes in related account balances, and management's experience with the control activity and/or the activity's history of errors and exceptions.

Leading companies determine their testing strategy considering the risk of control failure or the level of financial reporting risk. In considering the risk of control failure, management should think about the inherent reliability and importance of a control.

Key Insights	• **Inherent reliability of the control** – The risk that the control might not be effective. Inherent reliability is determined based on a consideration of a number of factors indicating a lower risk that the control would fail to prevent or detect a material misstatement. • **Importance of a control** – The risk that a material misstatement of the financial statements would result if the control failed to operate effectively (i.e., the risk that the control, either individually or in combination with other controls, would fail to prevent or detect a material misstatement on a timely basis, therefore, resulting in a material weakness).

Management's judgment will also depend on considerations related to:

- What to test (whether the controls reside among TLCs, ELCs or both), and how to test (the testing method that most effectively achieves the level and persuasiveness of evidence required to support management's assessment),
- Who does the testing, which depends on several factors, including auditor reliance considerations. But the higher the risk, the higher the degree of objectivity and competence required to conduct testing, and
- When to test, depending on the nature of the control and the judgment required. For instance, transaction-level controls that are subject to estimation and judgment should be tested towards year end.

The SEC Management Guidance offers management flexibility while emphasizing the importance of risk-based judgments in determining the appropriate testing strategy. A risk-based testing strategy should be a key objective for those companies that would like to reduce their overall costs of their 404 program.

Throughout the remainder of this section, "testing" refers to the procedures performed to obtain evidence about the operating effectiveness of controls. As discussed in the SEC interpretive guidance, the evidence that management evaluates comes from direct tests of controls, ongoing monitoring (which includes management's normal, recurring activities that provide information about the operation of controls), or a combination of both.

Varying the Nature of Testing

Determining the nature of the tests of controls involves several considerations: the nature of the controls, including the combination of ELCs and TLCs; the risk associated with the controls and the amount of evidence needed to determine that the controls operate effectively; knowledge of who will be performing the testing; and an understanding of the various parties who will use the results of the testing to support their conclusions.

Frequently, the nature of the control will determine the suitable testing techniques. For example, many TLCs can be easily tested by reperforming the control and determining that the control functioned effectively. However, some ELCs such as management reviews and monitoring are more subjective and might require gathering evidence of their effective functioning through a combination of inquiry, observation, and inspection of documentation. Where the risks associated with a particular control are lower and therefore

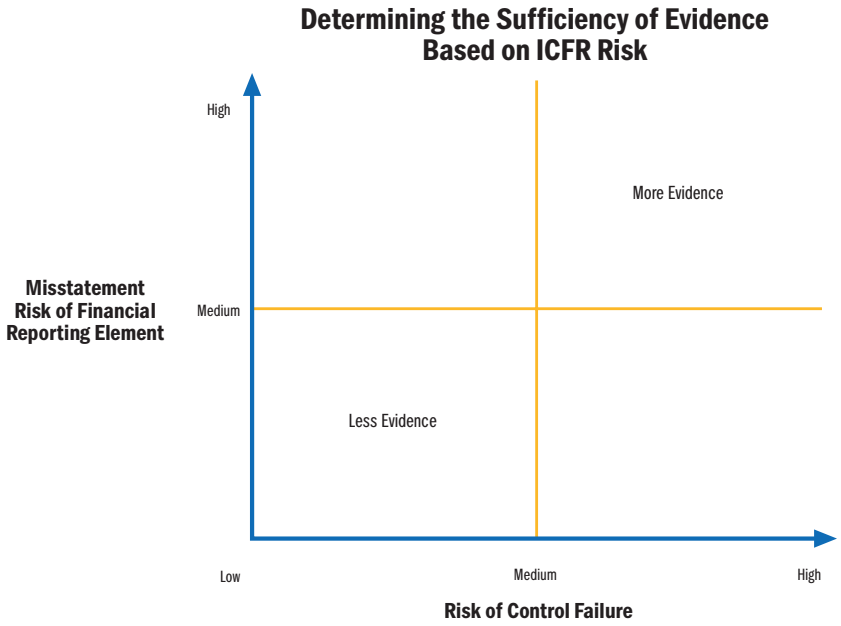
the amount of evidence needed to conclude that controls operate effectively is lower, testing techniques other than reperforming the control, such as evidence gathered through ongoing monitoring of direct or indirect information, might provide sufficient evidence of operating effectiveness.

Management's testing approach may involve one or more techniques depending on the risk associated with the control and the desired persuasiveness of the evidence. The desired persuasiveness of the evidence also should reflect the influence of indirect ELCs. While they may not correlate to specific financial reporting risks, they may have a positive influence on management's assessment of the reliability of the controls subject to testing. Also, benchmarking of automated controls may provide alternatives to testing large populations of TLCs.

The assignment of responsibility for control testing also should reflect the nature and risk associated with the controls. Where the risk associated with particular controls and the importance of the tests to management's evaluation is higher, there should be a commensurate increase in the competence and objectivity of those individuals performing the testing. Generally this is because it will require greater judgment to determine that the controls function effectively to address the risks. Therefore, assigning resources might involve critical judgment. It requires an understanding of the skills, capabilities, competencies, objectivity, and independence of those performing the work as this affects the persuasiveness of the evidence. Management also should consider the effect that the scope of its testing will have on the external auditor's strategy for the audit of internal control.

Varying the Timing of Testing

The SEC Management Guidance provides management not only with the flexibility to consider the persuasiveness of evidence needed to support its assessment, but also the opportunity to vary the timing of testing in response to the level of ICFR risk. Management has the flexibility to test controls during the year, and to perform update testing if necessary at year-end, based on consideration of the risk of control failure and risk that a material misstatement will occur in the event of a control failure. While management's assessment is as of a point in time, it is not possible, nor is it necessary, to perform all testing at or near the assessment date. For leading companies, their ongoing monitoring procedures and separate evaluations afford them greater flexibility. Ongoing monitoring assists in determining that controls continue to function effectively even though time has passed since the controls were subject to direct testing. The timing and frequency of the direct testing should reflect the risks associated with the significant account and related assertions and the risk associated with the controls, the influence of ELCs, and the strength of ongoing monitoring procedures and the evidence they provide.



The SEC Management Guidance emphasizes that the level of testing should vary with the level of ICFR risk, offering management an opportunity to adopt an effective testing strategy that considers the risks, costs, and value of the activity. For example, while some companies may choose to implement their testing strategies by hiring additional resources (thus adding to their annual fixed costs), leading organizations employ methods such as continuous control monitoring that may require upfront investments, but lower costs over the long term. Leading practices also indicate that considering the level of maturity of the control activity in determining its testing strategy can reduce costs even further, without compromising the effectiveness of the 404 process.

Key Insights	• Focus on and test only those controls that are needed to adequately address those risks that could lead to a material misstatement in the financial statements. • There is no requirement to identify, document, or test every control in a process impacting ICFR. • As assessed level of risk increases, vary the nature of evidence from ongoing monitoring to direct testing of controls and/or by adjusting the period of time covered by direct testing.
Questions to Consider	• Have you tested controls that are not required to support your assessment? • Is your testing strategy based on the persuasiveness of evidence determined to be necessary based upon the consideration of risk?

It is important to note that varying the nature, timing, and extent of testing may have an impact on the external auditor's use of the work of others. For example, management may perform less testing in an area that was previously relied upon by the external auditor. In this case, the auditor may need to perform additional testing, thus potentially raising external audit costs. Conversely, management testing that is performed by more competent and objective groups might provide the auditor greater ability to use more of management's work. In some cases, however, costs might fall for both management and the external auditor, for instance in low-risk areas where both management and the auditor are willing to accept less evidence than in previous years. Regardless of the approach, when considering efficiencies by varying the nature, timing, and extent of testing, management will generally want to take into account the impact on the external audit and then consider coordinating with the external auditor regarding their respective control testing strategies going forward.

Gathering Evidence

Management must determine the "body of evidence"—type and amount—to gather to support its assessment. Management also must decide how best to document the assessment together with supporting evidence (including considerations of format, volume, and specificity) as well as how much documentation to retain.

In the absence of clear guidance from the SEC, early efforts at implementing 404 often amounted to documentation "for documentation's sake" rather than the quality or persuasiveness of the evidence. The reasonableness standard described in the new SEC Management Guidance lends considerable flexibility to management in determining *what* it can test as well as *how* it does so.

Many formats and methods of documentation are permitted, clearly allowing management choices that can help to reduce the effort and cost expended on gathering and documenting evidence. As always, more evidence will be needed where the risk of control failure and material misstatement of the financial statements is higher. Where risk of control failure is lower, less evidence may be required. The point is that the evidence needs to be sufficient to support the conclusions of the ultimate evaluator—senior management. Since there are a number of key stakeholders in the process (i.e., external auditor, audit committee) there needs to be a well-thought-out plan for documentation that is sustainable over time and appropriate for the circumstances.

Under a top-down, risk-based approach, many companies may not need to maintain the amount of documentation of internal controls systems as in prior years. Management may discover cost-saving opportunities (with the caveat that control design documentation often supports other objectives of an effective system of internal control, such as the information and communication component).

Despite these opportunities to economize, management must weigh the needs and expectations of a variety of stakeholders when planning and implementing its assessment strategy. As we stated earlier, degree of risk and likelihood of control failure should drive management's decisions about the type of evidence to collect, how to collect it, who should collect it, how to document it, and how much documentation to retain. External auditor requirements—especially regarding the quality and specificity of evidence the auditor needs to meet professional standards and support the opinion on internal control over financial reporting—may also influence management's assessment strategy.

In the final analysis, however, no one is in a better position than management to understand financial reporting risks and related controls because of its day-to-day interaction with the business and ongoing monitoring activities. The SEC Management Guidance takes this special perspective into account in granting management the flexibility of a top-down, risk-based assessment approach. Management should consider this new flexibility thoroughly.

Key Insights	• Only gather evidence to support the evaluation based on the assessed level of ICFR risk. • Evidential matter such as daily interaction, self-assessment, and other ongoing monitoring activities may be sufficient to support portions of your evaluation. • Be careful not to cut back on work without considering the impact this would have on the sufficiency and quality of evidence supporting your conclusions and the effect on your external auditor's testing strategy.
Questions to Consider	• Did you vary the level of evidence to support the assessment based on the assessed level of risk? • Did you consider evidence that could be efficiently gathered through daily interaction, self-assessment, and other ongoing monitoring activities? • Did you consider external auditor reliance as a factor in determining your strategy for obtaining evidence?

Monitoring Controls

Monitoring of internal control helps to provide reasonable assurance to management that the organization's internal control system continues to operate effectively. Whether performed through ongoing processes or through separate evaluations, monitoring aids management in determining whether the right controls are in place and operating. Monitoring also aids management in identifying internal control deficiencies so that they may be reported to the right people and corrected in a timely manner. It is important to note, however, that while every control worth implementing is worth monitoring for effective operation, some controls inevitably are more important to monitor than others when management seeks to conclude on the overall effectiveness of the system of internal control.

The importance of monitoring a *particular* control depends on the significance of the underlying risk and the degree to which the control contributes to managing the risk. And, of course, monitoring can only be effective if there is baseline knowledge that underlying controls have functioned effectively at one point in time. Because many organizations have not had this baseline understanding, monitoring has heretofore not been an effective approach. But wherever this baseline knowledge is in place (such as through previous 404 program or related efforts), it can now provide the foundation for more reliance on monitoring activities.

While monitoring frequently is associated with entity-level controls, it occurs throughout an organization and its effectiveness depends on the persuasiveness of the information the monitoring provides. More relevant, reliable, and timely information is more persuasive and provides stronger support for conclusions as to the effective functioning of controls. Most people think of monitoring controls in the context of monitoring the results of operations (such as monthly reviews of financial performance, periodic budget-to-actual reviews). However, monitoring activities within an organization may provide some evidence of possible breakdowns in transaction-level controls. Generally this is a function of the design of the monitoring activities and their level of precision. For example, robust monitoring performed at sufficiently precise levels (such as regional, divisional, or individual business unit) can provide varying degrees of persuasive evidence as to the effective functioning of particular controls. Another factor affecting the relevance, and therefore the persuasiveness, of the monitoring is whether the monitoring activities involve direct monitoring of the functioning of particular controls or whether the monitoring is of other information (e.g., operating results, key metrics) from which management must infer as to whether controls continue to operate effectively. While both provide useful information, direct monitoring ordinarily provides more persuasive evidence about the operating effectiveness of controls.

Monitoring also serves to make sure that transaction-level controls are functioning on a continuous basis. A traditional example of the application of monitoring controls is evaluations by Internal Audit (IA) that are based on the objectives of IA's internal audit plan. The utility derived from an internal audit function does not reside in only one element of the control framework, but provides overlapping benefits. An effectively designed internal audit function is a reflection of the company's control environment, including the "tone at the top" and overall control consciousness. Management can leverage the internal audit findings to assist with its annual risk assessment, better understand the business issues it is currently facing, and adapt to the changing business environment in a timely manner.

Another more recent example of monitoring is the use of control monitoring tools. Control monitoring tools have for example, functionality that can automate the monitoring of controls to help detect control failure and improve control performance. While control monitoring tools and vendors have just emerged during the past few years with new products, management should consider the use of such tools when designing their testing approach as potential efficiencies could be obtained.

A final note about monitoring controls—The Committee of Sponsoring Organizations (COSO) is currently developing a white paper on the monitoring component of internal control. COSO's guidance in this area has the potential to improve every 404 program, especially in terms of cost, risk coverage, and value to the organization.

Look for recommendations from Ernst & Young in the near future as we add to our library of thought leadership concerning 404 program efficiency and effectiveness.

Closing Thoughts

It bears repeating that U.S. public companies have always had considerable latitude in determining how best to meet the reporting requirements of *The Sarbanes-Oxley Act of 2002*, including Section 404. In the uncertain early days of this legislation, many organizations erred on the side of caution when scoping the details of their planned assessment, just to be certain they had met all the requirements of the SEC and had full alignment with their external auditors. It now appears that this significant level of testing was greater than anticipated by the regulators. The most recent SEC Management Guidance has sought to refocus management on the key concepts of a top-down, risk-based approach and to highlight the significant flexibility management has in organizing its assessment process. Given these matters, let us summarize the observations and insights made in this document:

- The new SEC Management Guidance can impact organizations' 404 programs positively.
- It is to management's advantage to reassess its 404 program carefully, thoroughly, and critically.
- The SEC, recognizing best practices and lessons learned under the new law, encourages organizations to adopt a top-down, risk-based approach to planning and implementing internal controls assessments—and herein lies the key to rebalancing program cost, risk, and value.
- The top-down, risk-based approach makes possible a greater reliance on entity-level controls and emphasizes identifying the "right" combination of controls at the entity, process, and transaction levels in a way that addresses the cost of overly detailed testing focused primarily at the transaction level.
- Management needs to consider risk in determining the persuasiveness of the evidence needed to conclude that controls are effective.
- Automating portions of the testing of controls may help further to reduce costs and give greater assurance that controls are operating effectively.
- Depending on its current approach to assessing internal controls, management may want to transition portions of its 404 program to the more effective and efficient top-down, risk-based approach, or it may prefer to transform the program entirely.
- As always, management should stay aware of new developments in internal control guidance, design, and execution, such as updates from groups like COSO, and Ernst & Young will help management stay current with these developments.

Appendix

The appendices that follow are intended to help you assess the current state of your 404 program in light of lessons learned over the past several years, proven leading practices, and the SEC interpretive guidance; and, if necessary, to begin thinking about how to transform your 404 program to rebalance costs, risks, and value across the board.

We believe most U.S. public companies can improve their 404 programs. Ernst & Young offers these tools as a way for management to make a thoughtful start to the change process.

Appendix A: 404 Program Self-Assessment

To help organizations begin thinking about their 404 programs, Ernst & Young has developed the following 404 program self-assessment questionnaire. The continuum represented in the following page is designed to help management reflect on various program components and assess the quality of approach associated with each. The quality of approach continuum, therefore, represents a high-level assessment of an organization's opportunities to effect change:

- Leading Practice—among the leading practices of companies when addressing this aspect of their 404 program.
- Transition—an opportunity to modify the existing approach to Section 404 to gain additional efficiencies.
- Transformation—area of greatest potential for improving efficiencies within the 404 program.

404 Program Self-Assessment

		Transformation	Transition	Leading Practice
Transformation	1.) What criteria have you used to determine sufficiency of evidence?	AS2	Peer Analysis	SEC Guidance
	2.) How has the organization structured its resources to manage the 404 program effort?	No PMO/Ad-Hoc	Project	Program
	3.) How comfortable are you that your current 404 approach incorporates the necessary skills and knowledge to implement a top-down, risk-based approach?	Uncomfortable	Somewhat Comfortable	Very Comfortable
	4.) How would you assess the efficiency of your company's existing 404 processes?	Inefficient	Somewhat Efficient	Efficient
Top-Down, Risk-Based Approach	5.) What was your starting point in preparing the risk assessment?	Locations	Controls	Risks
	6.) What level of documentation did you develop and maintain for your 404 program efforts?	Exhaustive	Excessive	Efficient
	7.) What was the main factor driving your testing strategy?	Coverage	Control	Risk
	8.) To what extent have you leveraged shared services or other centralized processing?	No Leverage	Some Leverage	Full Leverage
Entity-Level Controls	9.) At what point in your process have you identified and evaluated ELCs?	End of Process	Middle of Process	Beginning of Process
	10.) To what degree have you leveraged your direct ELCs?	No Leverage	Some Leverage	Full Leverage
IT Controls	11.) Has the company effectively leveraged the use of application controls within the overall control population?	Ineffective	Effective	Highly Effective
	12.) How efficiently has the company employed a top-down, risk-based approach to identifying and testing ITGCs?	Inefficient	Somewhat Efficient	Efficient

404 Program Self-Assessment Explanation of Questions

The 404 Program Self-Assessment tool has been developed to help you thoughtfully consider various components of your 404 Program and identify opportunities for improvement. Each question has a spectrum of choices that correlate to the potential size of the opportunity for improvement. For your convenience, definitions are included for the various choices along the spectrum. For additional insights, contact your local Ernst & Young risk advisory professional.

		Transformation	Transition	Leading Practice
Transformation	1.) What criteria have you used to determine sufficiency of evidence?	AS2	Peer Analysis	SEC Guidance

Q1: What criteria have you used to determine sufficiency of evidence?

AS2: PCAOB Auditing Standard No. 2, which provided guidance for auditors on the audit of internal control over financial reporting until recently replaced by AS5, and until the issuance of the SEC interpretive guidance, was often looked to by management for guidance on the 404 assessment process.

Peer Analysis: Benchmarking studies, peer or industry networks, or other external sources measuring the extent of process and control documentation and testing required by management.

SEC Guidance: SEC Management Guidance, which permits management to take advantage of unique sources of evidence unavailable to others and to gear the evidence requirements to management's judgment based on its consideration of financial reporting risks.

		Transformation	Transition	Leading Practice
Transformation	2.) How has the organization structured its resources to manage the 404 program effort?	No PMO/Ad-Hoc	Project	Program

Q2: How has the organization structured its resources to manage the 404 program effort?

No PMO/Ad-Hoc: Decentralized governance of the 404 program effort. Often, a substantial amount of management assessment activity occurs at or near the end of the financial reporting year.

Project: 404 program activities are generally performed separate from other ongoing risk management and assessment activities in the organization. The 404 program activities receive inconsistent sponsorship from executives. The internal effort associated with Section 404 is treated primarily as a compliance exercise by the company.

Program: 404 program activities are fully embedded into recurring activities of the organization and are appropriately integrated with other risk management activities. In such an environment, there is a lower level of "404-specific" program activities that are performed. A 404 program receives the appropriate level of executive sponsorship and participation. Program activities occur throughout the year in support of management's annual assessment and quarterly certifications, and key business events that impact internal control over financial reporting are appropriately considered as they occur.

		Transformation	Transition	Leading Practice
Transformation	3.) How comfortable are you that your current 404 approach incorporates the necessary skills and knowledge to implement a top-down, risk-based approach?	 Uncomfortable	Somewhat Comfortable	Very Comfortable

Q3: How comfortable are you that your current 404 approach incorporates the necessary skills and knowledge to implement a top-down, risk-based approach?

Note: The SEC Management Guidance stresses the importance of involving the right people at key stages of the 404 process to effectively implement a top-down, risk-based approach. Specifically, such an approach requires sufficient knowledge of the business, its operation, organization and processes, the role of IT, internal and external risk factors, and the necessary understanding of the requirements of GAAP and its applicability to the underlying transactions.

Uncomfortable: The current program includes some of the above skill and knowledge elements at the right points.

Somewhat Comfortable: The current program includes many of the above skill and knowledge elements at the right points.

Very Comfortable: The current program included most or all of the above skill and knowledge elements at the right points.

		Transformation	Transition	Leading Practice
Transformation	4.) How would you assess the efficiency of your company's existing 404 processes?	 Inefficient	Somewhat Efficient	Efficient

Q4: How would you assess the efficiency of your company's existing 404 processes?

Inefficient: The current program includes documentation and/or assessment of controls and processes that, irrespective of the assessment results, would not meaningfully alter management's overall conclusion about ICFR effectiveness. Overall program resources may be misaligned and/or duplicative activities may be occurring. The extent of evidence produced is substantial and beyond management's requirements to support its assessment.

Somewhat Efficient: Changes have been made to the program in the years after initial implementation that have reduced the level of effort, including incorporation of elements of a top-down, risk-based approach. However, the overall level of effort is beyond what management considers necessary to support its assessment of controls. The program continues to incur significant hours in areas of lower risk.

Efficient: The allocation of program effort is closely aligned with the level of financial reporting risks in the organization. The extent of evidence produced is consistent with management's requirement to support its opinion and is focused on the most efficient and effective combination of controls and controls that is most readily assessable.

		Transformation	Transition	Leading Practice
Top-Down, Risk-Based Approach	5.) What was your starting point in preparing the risk assessment?	Locations	Controls	Risks

Q5: What was your starting point in preparing the risk assessment?

Locations: Our 404 program started by scoping locations based on size or other factors without considering the level of risk relating to material financial reporting elements.

Controls: Our 404 program started by looking at controls without considering the level of risk relating to material financial reporting elements.

Risks: Our 404 program started by determining financial reporting risks. This is the "leading practice" approach as it aligns controls and testing based on the level of risk.

		Transformation	Transition	Leading Practice
Top-Down, Risk-Based Approach	6.) What level of documentation did you develop and maintain for your 404 program efforts?	Exhaustive	Excessive	Efficient

Q6: What level of documentation did you develop and maintain for your 404 program efforts?

Exhaustive: Company has extensively documented processes and controls.

Excessive: Company describes all processes and controls related to Financial Reporting.

Efficient: Company selectively documents processes and controls related to Financial Reporting Risks.

		Transformation	Transition	Leading Practice
Top-Down, Risk-Based Approach	7.) What was the main factor driving your testing strategy?	Coverage	Control	Risk

Q7: What was the main factor driving your testing strategy?

Coverage: The organization's testing strategy was determined, and mainly driven by, the percentage of overall coverage of identified risks at locations with no regard to the level of risk at locations. Testing strategy is not tailored to address level of risk or location where risk resides.

Control: The organization's testing strategy was determined mainly by controls tested in the past and found effective in addressing risks identified, with little or no consideration to the level of risk, location of risk, and efficiency of control testing.

Risk: The organization's testing strategy was determined and mainly driven by the level of identified risk and the locations where these risks reside. Testing strategy, including the timing, extent, and nature of testing, is tailored to address the level of financial reporting risk and risk of control failure.

		Transformation	Transition	Leading Practice
Top-Down, Risk-Based Approach	8.) To what extent have you leveraged shared services or other centralized processing?	No Leverage	Some Leverage	Full Leverage

Q8: To what extent have you leveraged shared services or other centralized processing?

No Leverage: The organization has not leveraged a shared service model or centralized processing of transactions in its 404 program and has predominantly relied on transaction-level controls performed at decentralized locations.

Some Leverage: The organization has leveraged some shared service functionality or centralized processing of transactions but still has some controls performed on a decentralized basis.

Full Leverage: The organization leveraged a shared service model or centralized processing of transactions and assessed the efficiency and extent of reliance that can be placed on those controls.

		Transformation	Transition	Leading Practice
Entity-Level Controls	9.) At what point in your process have you identified and evaluated ELCs?	End of Process	Middle of Process	Beginning of Process

Q9: At what point in your process have you identified and evaluated ELCs?

End of Process: Identify and evaluate ELCs late in the evaluation process. Typically, this will not allow companies enough time to determine the degree of leverage ELCs may offer in reducing the level of TLC testing and the level of 404 program costs.

Middle of Process: Identify and evaluate ELCs in the middle of the evaluation process. This may allow management some time to determine the degree of leverage ELCs may offer in reducing the level of TLC testing. However, the timing may likewise result in missed opportunities as some TLC testing may have already been completed.

Beginning of Process: Identify and evaluate ELCs at the beginning of the process. This is beneficial because it allows an organization to see how far the more pervasive ELCs can assist to address risk and reduce the level of TLC testing required to obtain an appropriate level of comfort.

		Transformation	Transition	Leading Practice
Entity-Level Controls	10.) To what degree have you leveraged your direct ELCs?	No Leverage	Some Leverage	Full Leverage

Q10: To what degree have you leveraged your direct ELCs?

No Leverage: The organization has not leveraged direct entity-level controls in its 404 program and has predominantly relied on transaction-level controls.

Some Leverage: The organization has leveraged some direct entity-level controls to the extent the organization relied upon controls residing in the financial statement close process, analytics and analysis, and other direct entity-wide controls in its management assessment. The organization has not gone through the thought process in identifying the most efficient controls to test.

Full Leverage: The organization went through the thought process of identifying direct entity-level controls and assessing the efficiency and extent of reliance that can be placed on those controls.

		Transformation	Transition	Leading Practice
IT Controls	11.) Has the company effectively leveraged the use of application controls within the overall control population?	Ineffective	Effective	Highly Effective

Q11: Has the company effectively leveraged the use of application controls within the overall control population?

Ineffective: The organization has not leveraged application controls in its 404 program and has predominantly relied on manual controls.

Effective: The organization has identified some application controls. However, the organization has not done an assessment to identify the most efficient controls to test.

Highly Effective: The organization has performed an assessment to identify the most efficient controls to test, including the extent of reliance on application controls.

		Transformation	Transition	Leading Practice
IT Controls	12.) How efficiently has the company employed a top-down, risk-based approach to identifying and testing ITGCs?	Inefficient	Somewhat Efficient	Efficient

Q12: How efficiently has the company employed a top-down, risk-based approach to identifying and testing ITGCs?

Inefficient: The organization has identified and tested ITGCs for all financial applications without considering risk.

Somewhat Efficient: The organization has identified and tested ITGCs for all applications that support significant classes of transactions. However, the organization has not done a detailed assessment to identify the most efficient ITGCs to test and rely upon.

Efficient: The organization has gone through an assessment to identify and leverage the most efficient ITGCs to test and rely upon.

Appendix B: 404 Transformation Approach

The Transformation Objective

The objective of a Section 404 transformation program is to implement improvements to an organization's 404 program that are consistent with SEC Management Guidance and the organization's goals. The transformation includes reassessing scope, approach, roles and responsibilities, and considering lessons learned from management's own experience and that of others. Companies seeking substantial improvement upon current 404 program practices may want to think about fully transforming their programs. Others may feel satisfied with current-state practices but still seek incremental improvements on a case-by-case basis.

To assist in developing and implementing the right 404 program for the organization, Ernst & Young has developed the following structured approach.

An Ernst & Young risk advisory professional can work with you to explore the details of this approach at your convenience.

ERNST & YOUNG LLP www.ey.com

SCORE Retrieval File
No. DY0002