

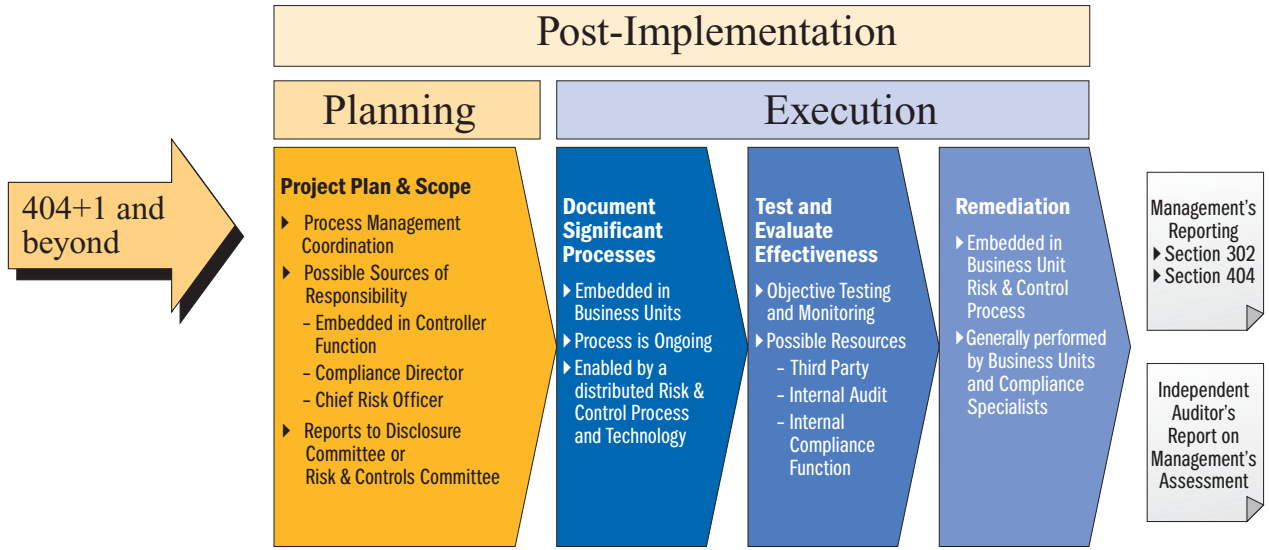
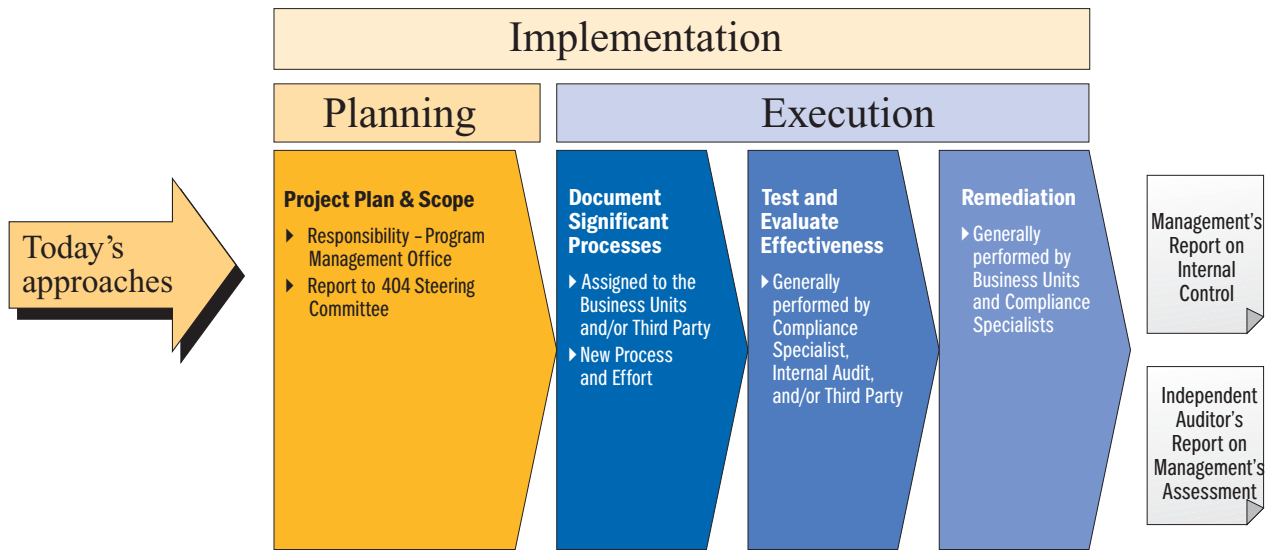
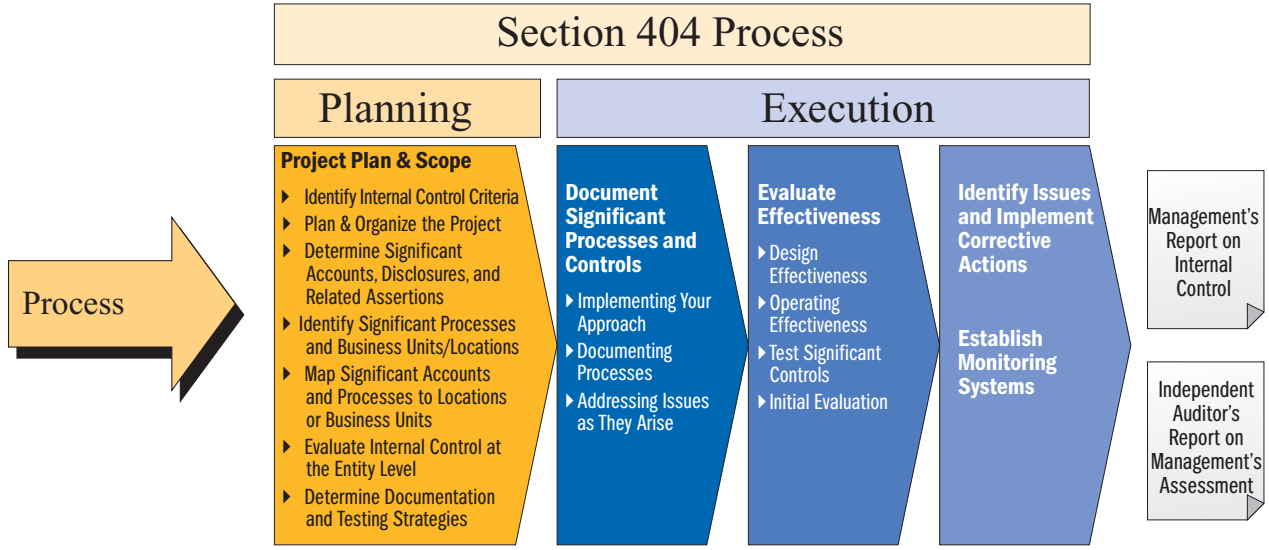


 **ERNST & YOUNG**

Quality In Everything We Do

Section 404 Post-Implementation

What You Should Be Thinking About Now



To Our Clients and Friends

Companies are in the midst of implementing Section 404 of the Sarbanes-Oxley Act of 2002 (Section 404), one of the most involved and costly processes they may have faced. As Ernst & Young continues its ongoing process of surveying companies to gather information on leading practices for approaching Section 404 compliance, we will analyze and distribute that valuable information to you.

Many companies are starting to think past implementing Section 404 to post-implementation—“404+1” and beyond. We work with companies to help them address post-implementation issues: level of effort, how to embed control consciousness in business units, and how to avoid being locked into “implementation-only” strategies that may prove to be cost-ineffective in the long run.

While we recognize the significant time and effort your company is putting toward Section 404 *implementation*, we feel strongly that *post-implementation* is something you should be thinking about *now*. The requirements of Section 404 are no less onerous in year two and beyond, although the sheer amount of documentation may be less.

Based upon surveys we have conducted, as well as observations from Section 404 Roundtables and seminars, we have noted some preliminary observations on 404+1:

- ▶ Ongoing compliance efforts will be significant—as much as 50% to 75% of first-year implementation.
- ▶ Over 70% of companies are planning some form of control self-assessment as part of their future compliance strategy, yet many such programs have failed to deliver in the past.
- ▶ The role of internal audit in the ongoing process is still evolving, and views seem to be polarizing.
- ▶ Technology enablers and other techniques can reduce the cost of compliance and bring additional value.

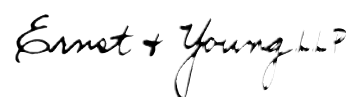
In this brochure, we focus on:

- ▶ Differences and similarities between implementation and post-implementation years.
- ▶ Approaches to managing the ongoing process.
- ▶ Approaches to documenting areas of change.
- ▶ Ongoing testing efforts and resources.
- ▶ The role of internal audit and other risk functions.
- ▶ Extracting value from the process.

We also present a possible framework for the future, containing many of the elements we are developing and piloting with a select group of companies.

Leading companies recognize the importance of laying the groundwork for 404+1. Ernst & Young will continue to observe and analyze emerging issues around Section 404 and will provide periodic updates to you to help make your path clearer and more predictable.

To provide comments, ask questions, or obtain additional information, contact Tom Bussa, global director of Business Risk Services, at Thomas.Bussa@ey.com or your local Ernst & Young office.

The logo for Ernst & Young, featuring the company name in a stylized, cursive script font.



Introduction

Many companies are currently in the throes of completing documentation and testing of controls to satisfy the initial-year reporting requirements of Section 404. Other companies are focusing efforts to remediate situations where controls are missing, not designed properly, or not functioning as intended.

As the reporting season nears, CFOs are looking forward to the time when, following the report from their external auditor, they can put the entire experience behind them and move on. Frustrated executives talk more frequently about the need to get “back to business”—to redirect their energy to increasing shareholder value and growing the business.

As a result, this may seem like the worst time to think about what needs to be done in the years following what has been, for many, a time-consuming and expensive compliance exercise. However, for a number of reasons, now is precisely the right time to begin to think and talk about it.

The Public Company Accounting Oversight Board (PCAOB) requires that each year’s Section 404 compliance effort “stand on its own.” Therefore, each year you will need to determine your significant accounts and relevant assertions, update documentation for significant processes and controls, assess design effectiveness, test controls, and remediate any issues in order to evaluate operating effectiveness and issue management’s report. In post-implementation years you will also need to evaluate any change during a fiscal quarter in the company’s internal control over financial reporting that has materially affected, or is reasonably likely to materially affect, the company’s internal controls over financial reporting. Management will need to certify that it has performed this evaluation as part of its quarterly certification under Section 302 of the Sarbanes-Oxley Act of 2002 (Section 302).

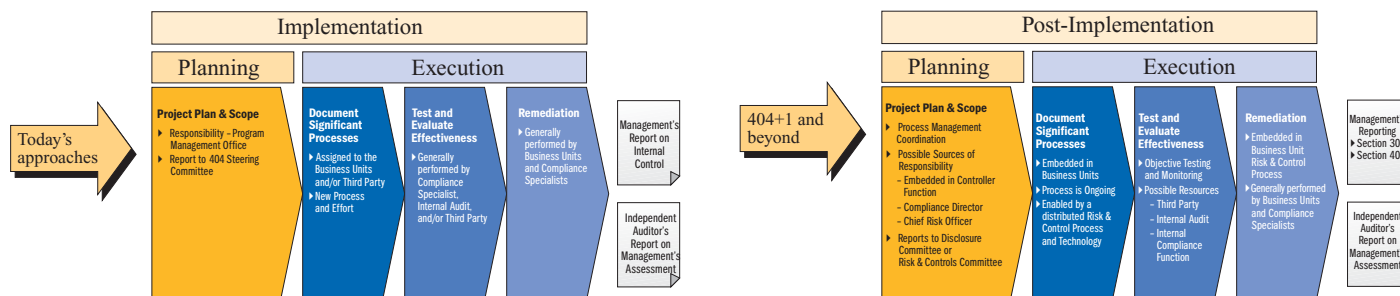
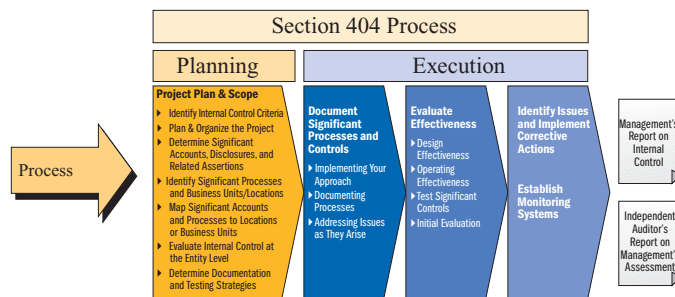
The key to post-implementation effectiveness and efficiency will be to appropriately address each activity and to develop a framework under which the company continually operates.

Overview

Let's start by understanding the similarities and differences between the processes and efforts required for Section 404 implementation and post-implementation years. The diagrams on this page provide a good framework from which to start.

Most companies' Section 404 process is reflected in this diagram and consists of five key activities: 1) Project Plan & Scope, 2) Document Significant Processes and Controls, 3) Evaluate Effectiveness, 4) Identify Issues and Implement Corrective Action Plans and Establish Monitoring Systems, and 5) Management's Reporting.

The following diagrams summarize typical implementation and post-implementation processes.



Currently, Ernst & Young is assessing overall levels of effort in post-implementation periods as compared with initial implementation. Many factors, including system changes, level of control consciousness, centralized versus decentralized systems, business expansion or contraction, and other projects in progress, will affect the level of comparative effort. All things being equal, we believe each year's post-implementation effort could be 50% to 75% of your initial implementation effort.

The Project Plan & Scope effort in the implementation year was significant. Companies found almost everything new, unfamiliar, and in need of being created. They had to assess new regulations and adapt them to their organizations; assess, identify, and obtain resources; and carry out all necessary project planning, monitoring, and coordination efforts. Project leaders were identified and Project Management Offices (PMO) established with responsibility to complete the project. The PMO often reported to a 404 Steering Committee. The 404 Steering Committee typically comprised a cross-section of stakeholders in the process, including elements of the Section 302 Disclosure Committee.

In post-implementation years—404+1 and beyond—the Project Plan & Scope effort should not be as great, but you will still need to carry out many of the same activities. The overall process—determining significant accounts and disclosures and relevant assertions, identifying significant processes and locations, and updating the relevant documentation and testing strategies—will have to be conducted each year. Finally, coordinating and monitoring the process is still necessary. If implemented correctly, the PMO will become a process management effort that requires continuous, focused leadership.

Documenting Significant Processes is necessary each year. Developing documentation for new or changed areas, or updating documentation to take into account changes in the business (e.g., major new systems, processes or acquisitions), will require the majority of effort, but you will need to evaluate systems, including those that didn't change, to determine they still function as designed.

Testing and Evaluating operating effectiveness of the significant processes will not change much from implementation to post-implementation. You may gain efficiencies from experience and use a streamlined combination of alternative testing and monitoring efforts, but the bulk of the effort will be the same each year.

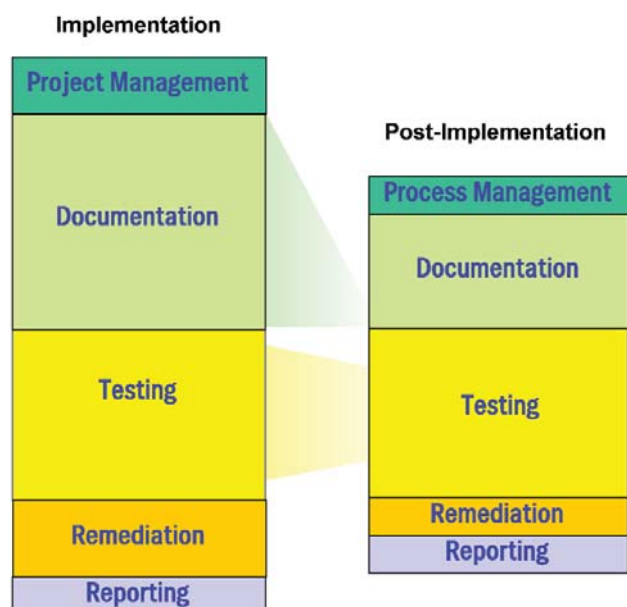
Remediation should be greatest in the implementation year, but it would be unreasonable not to assume that remediation will be necessary to address a certain level of control failure or improvements each year, especially in areas that have changed.

Last, in post-implementation years, you will need to link ongoing Section 404 monitoring efforts to quarterly reporting under Section 302. Section 302 requires quarterly evaluation and reporting of any changes in internal controls over financial reporting that either have or could have a material effect on the financial statements. Accordingly, companies must develop the ability to keep their assessment of internal controls over financial reporting “fresh” throughout the year and cannot wait until the end of the ensuing fiscal year to evaluate changes in internal control for their annual assessments.

Obvious questions begin to present themselves:

- ▶ Who will manage the process going forward?
- ▶ How do we address ongoing documentation?
- ▶ Who will do the testing?
- ▶ What is the role of internal audit and other risk functions?
- ▶ What enablers or tools can be used to make the process as efficient as possible?
- ▶ Can any value be extracted from this process?
- ▶ How do we evaluate changes occurring during the quarter?

Levels of Effort



Post-Implementation Considerations

PROCESS MANAGEMENT COORDINATION

It is vital that companies establish ongoing processes before skilled resources in the PMO and project teams are allowed to resume their previous responsibilities or take on new roles unrelated to Section 404. Otherwise, the significant investment in their education and skill development may be lost.



Where should ongoing process management responsibility reside? Several possibilities have been identified.

- ▶ Most commonly discussed is embedding ongoing Section 404 process management coordination in the controller function. This process is, after all, a financial controls-based activity aligned to quarterly and annual reporting. The controller's functions are located within the business units and overall financial reporting responsibility is usually within this group. Therefore, it seems to be the most logical fit.
- ▶ Some organizations may opt to create a compliance function, outside the controller group, similar to those found in many regulated industries. Such a group may act as an internal consultant to the business units, as well as a monitoring function able to provide senior management with objective assurance over design and operating effectiveness. In this type of model, companies believe a smaller in-house process management function, coupled with outsourced compliance testing, could provide the most effective allocation of resources.
- ▶ Other organizations are looking to tie process management coordination to the ongoing objective testing and monitoring aspects of the process and assign overall responsibility to their chief risk officer.

The process management function requires organizational reporting protocols, clearly articulated responsibility, and accountability. Two main schools of thought are emerging. Some companies are considering converting their existing Section 404 Steering Committee to a Risk & Controls Committee (RCC) to help maintain the appropriate "tone from the top." Such an RCC would be represented on the company's Disclosure Committee, thereby tying in Section 404 and Section 302 efforts. Other companies are not considering the RCC concept, but would have process management report directly to the Disclosure Committee.

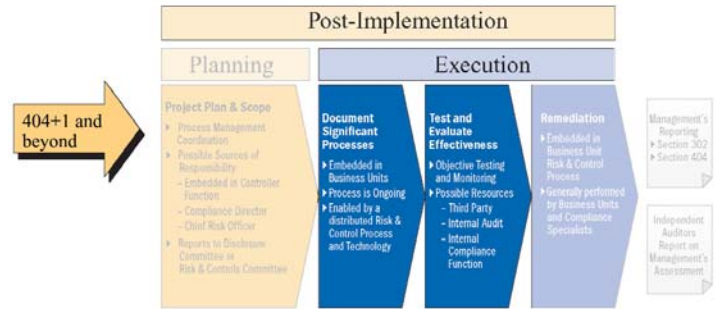
Key Points

Process Management Coordination:

- A plan must be implemented to migrate existing PMO and project team knowledge effectively into your ongoing process management coordination.
- Some companies are assigning ongoing responsibility to the controller's function; some are creating a compliance function; and others are assigning overall responsibility to a chief risk officer.
- A Risk & Controls Committee or Disclosure Committee may be used to organize the process, define responsibilities, and establish and manage the reporting process.

ONGOING DOCUMENTATION AND TESTING

The PCAOB requires each year’s assessment to stand on its own. Initially, post-implementation testing may not yield significant reduction in time and effort. Incremental changes in your underlying processes, better controls around the IT environment, and maximizing reliance on IT-based controls could provide worthwhile savings as time progresses.



Many companies believe that the documentation of new and changed processes, as well as continual design effectiveness assessment, should be embedded in the business units. In their view, using elements of control self-assessment and requiring process owners to maintain documented support as to design effectiveness and routinely to address changing risks and controls, places responsibility where it should be.

For many companies, Section 404 implementation introduced this documentation process. In post-implementation periods, we believe documentation will be most effective and efficient if supported by a risk and controls process methodology and enabled by distributed technology.

Control Self-Assessment Technique

Many companies are implementing control self-assessment as a technique to distribute responsibility for managing the documentation and assessment process to the lowest level and to allow for an assertion “roll-up” on a quarterly and annual basis. This approach involves assigning responsibility for the controls to the process or control owner, who is then held accountable for assessing its design effectiveness and, to a lesser extent, assessing operating effectiveness.

Potential advantages of this approach include:

- ▶ Improved quality, as the people managing the process are better able to provide ongoing assessment of the process.
- ▶ Increased control consciousness, as ownership, responsibility, and accountability for controls is made explicit.
- ▶ Basis for real-time identification of process and business changes.
- ▶ Reduced cost: a large centralized function is not necessary. Process owners add these activities to their existing responsibilities.

However, there are potential issues:

- ▶ Open culture that supports such an introspective process may be missing.
- ▶ Potential inherent lack of objectivity. Auditors will not rely on the “self-testing” aspect.
- ▶ Need for ongoing objective monitoring.

A first-time self-assessment survey is most likely completed with due care and rigor. However, answering the same questions the third, fourth, and fifth times may not generate the necessary levels of effort for a proper assessment. A good first-year project can quickly turn into a mundane form-completion exercise that provides only the illusion that documentation is current and controls are being monitored.

Supplemental Approaches

Because of its limitations, self-assessment alone generally will not provide management with sufficient evidence that controls are effective. Self-assessment should be coupled with objective testing and monitoring of controls performed separate from the process owners. Also, external auditors can rely more on objective testing than on self-testing.

Some companies are exploring approaches designed to reduce the cost of compliance by capitalizing on management's normal review activities. For example, when a controller periodically reviews the work of a junior credit clerk, he or she looks for evidence that the proper controls—for instance, the follow-up of past due items—are being performed effectively. For this approach to work, management must document that the review was carried out to provide satisfactory evidence that the control operates effectively. Many supervisory activities rely only on making inquiries, which are not a sufficiently reliable basis for management to make its assertion as to control effectiveness. Inquiries must routinely be supplemented by observation and inspection (e.g., inspecting evidence that the appropriate reviews were performed, or direct observation of the functioning of the control to prove it has, in fact, operated). For supervisory reviews and monitoring to be sufficient for the external auditor's reliance, it should support and reflect the importance placed on the control and the frequency with which the controls function.

We believe that basing the control evaluation on management's ongoing supervision may require significant changes in the way management operates. Technology solutions may help with the evidence-gathering process, but the degree of work should not be underestimated.

A common management letter comment from external auditors identifies lack of adequate controls around a company's program change controls over IT processes. Oftentimes, companies have not expended time or money to fix this control process. In today's environment, IT processes could be an effective way of reducing testing costs. If you do not have an effective program change control process, you will need to test every IT control upon which you rely each year. If you have an effective program change control process, you can test this control process and benchmark IT controls that have not changed (you will not need to retest underlying controls that have not changed). Therefore, the more you can "push" control reliance back into your IT environment, the more you can reduce your testing effort.

Who Will Test?

Another challenge companies will face post-implementation is who will perform objective testing. Possible resources include a third party, internal audit, or an internal compliance function.

U.S. and accelerated filers have had most of 2003 and 2004 to prepare for reporting under Section 404. Foreign private issuers will have 2005 and possibly some of 2006 to prepare. During post-implementation, however, everyone will be required to complete the entire process each year. You will probably want to minimize roll-forward time, but you also will need an acceptable period for any remediation issues. For 31 December year-ends, your main testing probably will be condensed to June–August/early September (January–February/early March in the Southern Hemisphere where 30 June is the most common year-end) with vacations/holiday periods during the same time frame. This will maximize your resource requirements necessary to complete testing on a timely basis. In addition, you will need to perform adequate roll-forward procedures. Many

companies have concluded that a combination of effective processes, better IT reliance, and third-party resources will be essential to minimizing costs of ongoing testing.

Initially, post-implementation testing may not yield significant reduction in time and effort. However, incremental changes in underlying processes, better controls around the IT environment, and increased reliance on IT-based controls could result in worthwhile savings. This is discussed in more detail later.

Key Points

Ongoing Documentation and Testing:

- Post-implementation documentation will likely be most effective and efficient if supported by a risk-and-controls process methodology and enabled by distributed technology and responsibility assigned to the process owners.
- While many companies are using control self-assessment, it should be coupled with objective testing and monitoring of controls implemented separate from the process owners.
- Some companies may reduce the cost of compliance by leveraging management's normal review activities (e.g., inquiries, observation, inspection).
- Effective program change controls over IT processes can reduce testing efforts.
- A combination of effective processes, better IT reliance, and third-party resources will be the key to efficient ongoing testing.

THE ROLE OF YOUR INTERNAL AUDIT AND OTHER RISK FUNCTIONS

Internal audit's role to provide objective reviews of how risks are being managed makes it an obvious choice for carrying out ongoing Section 404 testing. In many cases, internal audit functions have filled this role during implementation. Internal audit can also be important to the company's internal control structure as a result of its monitoring role.

However, the trend over the last 10 years has been for internal audit to focus more on operational auditing than on financial reporting. Accordingly, their reviews are more often focused on business processes rather than financial processes, and internal audit functions have developed consulting and operational skills rather than traditional audit skills.

At a recent Institute of Internal Auditors conference, we informally polled general auditors on how they view their role in post-implementation. Their positions were evenly split between direct involvement in the post-implementation process and either remaining at arm's length or totally separate from the process in order to be an objective reviewer of the process. The discussion elicited a strong emotional response regardless of position.

You will need to consider and evaluate the role of your internal audit function. Prior to Section 404, most companies properly had their internal audit function focusing on a wide variety of key strategic, operational, and/or financial risks. If you now focus a significant portion of your internal audit's effort on Section 404 financial controls, how can you address the other risks and audit plan activity previously considered significant by internal audit, management, and the audit committee? To cover all these areas, companies' expenditures for risk functions and activities necessarily will increase.

If internal audit is to play a key role in the future of Section 404 compliance, management and/or audit committees also will need to reconsider the mix of skills within many departments. Resources may have to be supplemented to address both business risks and the requirements of Section 404. For this reason, it may not

make sense to house the financial controls compliance function within internal audit, but instead to operate a separate group or outsource it to a third party, perhaps reporting directly to the audit committee.

Most companies have other risk functions or groups to which risk management issues are assigned, including risk management departments, general counsel’s office, tax departments, and IT departments. Their use in post-implementation will vary depending on the skills needed, the processes they already own, and the level of objectivity they can contribute to the process. The general counsel’s office usually participates in certain judgmental processes; tax departments and IT departments will have many specifically needed skills but will offer little objectivity in their related processes; and enterprise-wide risk management functions usually are involved in designing and implementing risk management-related systems. You will need to weigh the benefit (through reduced costs) of using internal skill sets against any inherent potential for lack of objectivity and the reduced level of reliance external auditors may place on their work.

Key Points

The Role of Your Internal Audit and Other Risk Functions:

- Companies must reconsider and reevaluate the role of their internal audit function post-implementation.
- If internal audit is to play a key role in Section 404 compliance going forward, management and audit committees will need to reevaluate the company’s overall resource skill mix.
- Companies’ expenditures in risk functions and activities necessarily will increase.

THE ROLE OF TECHNOLOGY ENABLERS

Technology tools can play a key role in the ongoing Section 404 compliance process. Companies that currently are selecting a technology enabler need first to develop a clear idea of the ongoing process they want to create before investing in a tool that may not support future development. Misinformed purchases can be costly, not only in terms of technology acquisition cost, but also in the time and effort required to transfer data, retrain users, and establish new ways of working.

EXTRACTING VALUE FROM THE PROCESS

After implementation, companies will have a complete catalog of financial controls and an understanding of the functioning of myriad financial processes—many for the first time. This documentation and in-depth understanding can provide a basis for deriving real value from the process. With appropriate focus, management may be able both to reduce the cost of internal control and the cost of ongoing compliance.



Many companies will be focusing on value opportunities in the first post-implementation year:

- ▶ First, they will address redundant controls. Controls often evolve over time without reference to other controls because no one has been able to see or assess the “big picture.” It is human nature to establish controls over activities for which an individual is responsible. Each manager tends to establish controls so that he or she can be confident of the validity and accuracy of transaction processing, apart from controls imposed at higher levels or in different parts of the system. Now the list can be fine-tuned, the processes refined, and unnecessary controls and costs removed.
- ▶ Second, they will seek to improve the balance of control—possibly combining controls more effectively to prevent errors. This could take the form of more reliance on prevent- rather than detect-type controls or more systematic versus manual controls. Also, as discussed earlier, this can mean greater reliance on IT systems, since significant savings may be gained from automated controls, provided systems are secure and stable. By having business processes mapped to IT application processes, you can identify system-critical controls along with potential flaws in the controls process. This will allow you to focus on leveraging IT application controls to their fullest.
- ▶ Third, they will seek to improve controls to remove “noise level” errors. Although they may not be material from the perspective of the financial statements, such errors can nevertheless represent significant rework costs. Building additional controls may be cost-justified in terms of the alternative cost of reprocessing transactions or lost overall process time, and improvements in customer satisfaction.

Better integration of the financial controls evaluation process into the way changes are managed also may save significant expense. For instance, embedding a requirement to build and at the same time document financial controls in new systems under development from inception through implementation and testing will be much less costly than documenting and adding controls to the system once it has been rolled out.

Another likely benefit of establishing a sound infrastructure for internal controls as a result of Section 404 will likely be the ability to expand coverage from financial statement controls to controls that enable the business to operate more effectively. Controls over compliance with applicable laws and regulations, as well as controls that address everyday operational effectiveness, are two examples.

Key Points

Extracting Value from the Process:

- Management may be able to both reduce the cost of control and the cost of ongoing compliance.
- Better integration of the financial controls evaluation process into change may cut costs significantly.
- The ability to expand from financial statement controls to controls that enable the company to operate more effectively is a tangible benefit.

A Model for the Future

Continuous monitoring technologies, control self-assessment frameworks, and dashboard reporting tools can be integrated to offer cost-effective, comprehensive control management and monitoring systems to organizations. Core components of such systems have been operating in companies for several years. For example, many banks monitor transaction data in real time in order to detect credit card fraud. Supply chain companies have more recently embraced the need to perform real-time monitoring of transactions to identify bottlenecks before they cause serious damage to operations.

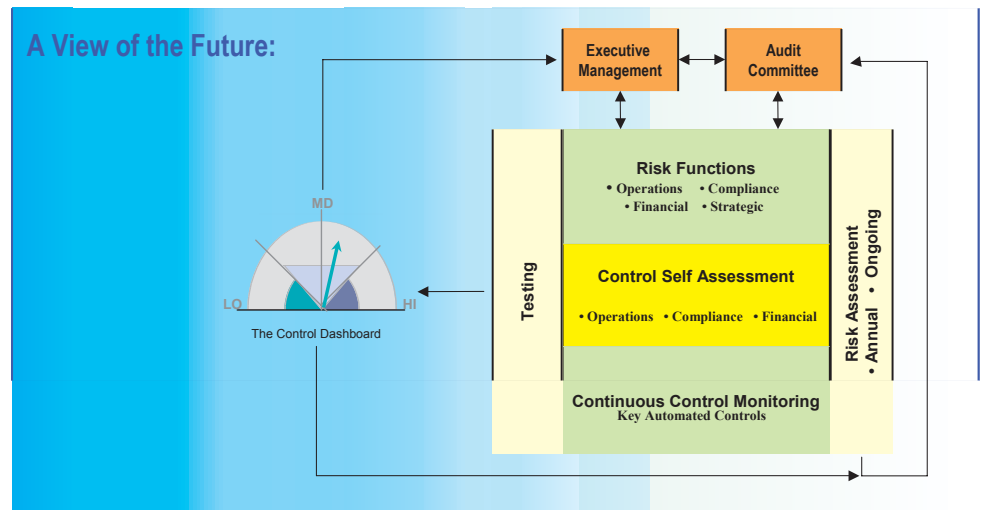
We are developing an initial “model of the future” that includes:

- ▶ Combination of integrated continuous monitoring technologies for:
 - Application-level changes in segregation of duties and changes in the detailed configuration of application controls.
 - Ongoing functioning of application and manual controls.
- ▶ Control self-assessment with both “active and passive elements.”
- ▶ Comprehensive assessment, monitoring, and enhancement methodology aligned across all business units and activities.
- ▶ Risk function investments and activities aligned with and linked to continuous control monitoring and control self-assessment processes.
- ▶ Continuous reporting to senior management and, as appropriate, the audit committee.

Continuous control monitoring is a technology-driven opportunity. It works best once an effective change control process exists in your IT environment. First, technology can be used to monitor application-level changes in segregation of duties and changes in the detailed configuration of application controls. Once an effective environment has been established, process owners can monitor changes to this base level through passive and active self-assessment. For example, process owners are notified of changes in the set-up of application controls, including whether or not they are turned on or can be bypassed, so they can assess the effect of these changes and remedy any control weaknesses.

Second, technology can be used to monitor the ongoing functioning of application and manual controls to provide, in effect, 100% testing, with automated alerts of potential control failures routed to the responsible people. For example, let’s assume a purchasing control is “*all goods are ordered from an approved price list.*” There may, however, be multiple reasons why an order may be made at a different price. Accordingly, you may have determined that, if you order from the approved price list at least 95% of the time, the control is probably working. You can use technology to monitor every instance in which this control should function, and, if non-compliance exceeds 5%, the process owner(s) can be notified that the control is not working. This then prompts the process owner to assert whether the control(s) does in fact operate correctly and, if so, to explain the data anomaly. The control self-assessment process now becomes more active; there is a presumption of control failure that must be rebutted by management.

These technologies should be linked to self-assessment processes and to internal audit risk assessments allowing the actual effective rate of controls to be used in the periodic self-assessments and in assessing broader risk in the organization. They permit a prompt, objective review of any area in question. For example, internal audit or a compliance function could use the output to verify the validity of related control assertions.



Next, a control self-assessment process should be a part of your control environment. This allows you to most effectively assign and embed the process control responsibility and ongoing Section 404 effort with the business units and process owners. In a separate survey we conducted in April 2004, over 70% of all companies planned to adopt some form of self-assessment process post-implementation.

For self-assessment to be effective, you will need: 1) appropriate technology, 2) methodology aligned to other risk-based activities (e.g., internal audit, risk management), 3) common documentation and assessment criteria, and 4) objective testing of the self-assessment activities and conclusions.

The activities of your risk functions need to be linked to the underlying elements of this model in addition to their other processes, technology, knowledge, and training enablers. By incrementally investing in the underlying tools, more effective risk assessment is possible, including the ability to change the risk assessment and related audit plan objectively, based upon the underlying monitoring and mitigation of financial, operating, regulatory compliance, and strategic risks. This in turn will promote the most effective allocation of resources.

Under this model, activity is monitored, and dashboard reporting allows senior management and, as appropriate, the audit committee to monitor and act—as opposed to react—to control and mitigation issues. The entire process is reviewed periodically to assess any new risks and to take account of systems and process changes.

The benefits of such an approach are numerous. We also expect this model to allow external auditors to place greater reliance on overall control processes. Ernst & Young currently is piloting this approach with Fortune 100 Section 404 advisory clients.

Conclusion

The requirements of Sarbanes-Oxley are here to stay. In order to avoid making costly mistakes today, companies must begin thinking about and focusing on the future state of their compliance *now*. Management must consider the skill sets required, the overall approach, and the possibility of extracting real value from the process.

We hope we have helped you identify potential implementation and eventual post-implementation issues. We remain available to help you address these issues in your company.

ERNST & YOUNG

www.ey.com

Copyright © 2004 EYGM Limited.
All Rights Reserved.

SCORE Retrieval File
No. AN0092