# How to move your company to sustainable Sarbanes-Oxley compliance—from project to process*

PwC Advisory
Performance Improvement

# Table of Contents

# Situation
## It’s time to learn from first-year compliance

For most U.S. public companies, the first year of implementation and reporting under Section 404 of the Sarbanes-Oxley Act of 2002 (Sarbanes-Oxley) is over. Those who took on the task found that it was by no means a small one; rather, it required a significant investment of management time, resources and money. Many business leaders are, however, quick to acknowledge the value of operational insights gained during the process. As they look beyond their first-year experience, these leaders are now faced with an important question: how to develop a sustainable way to remain in compliance with Sarbanes-Oxley.

It is a crucial question. Each organization will need to find its own answer—sustainable Sarbanes-Oxley compliance being a careful mix of economic viability, social responsibility and sound operations. Company leaders wrestling with this question share a common challenge: the need to quickly determine and implement a process that is cost-efficient, fully conforming with Sarbanes-Oxley regulations and operationally effective.

Attaining cost-efficiency and effectiveness in Sarbanes-Oxley compliance is a necessary as well as worthy goal. Since the legislation took effect, the business community striving to meet its requirements has shown evidence of frustration. Among the reasons:

- Management, in many cases, did not initially understand the scope of Section 404 and its far-reaching effects on business units, financial statement accounts and significant processes—a breadth and depth of control documentation and evaluation that were considerable. Management teams and employees lacked thorough implementation guidance, and many companies found that they were either doing too much or too little.
- Management, at times, did not anticipate the amount of remediation to be completed. Not only were fixes needed to improve the operational effectiveness of controls, but there was also the matter of deferred maintenance on basic internal controls impacting financial reporting that needed to be addressed. Process and system documentation were found to require a significant amount of updating, and in many cases, documentation had to be created from scratch.
- Levels of expertise required to implement Section 404, including control design assessment, documentation and control testing, were underestimated. Requisite skill sets were not in abundance; in some cases, they were not even in-house. Scarce resources required management to divert the attention of many employees, including Internal Audit personnel, from their normal job responsibilities in order to focus on first-year activities. In many instances, management engaged third parties to assist with the effort, bolstering technical resources at hand but increasing cost along the way.

A natural response to these issues for many organizations was to address Sarbanes-Oxley requirements as a discrete project. First-year Section 404 compliance, in fact, was all about project management, with companies organizing teams to:

- Identify significant business units, financial statement accounts and related processes
- Update or create process-flow documentation
- Assess risks related to financial reporting and identify control activities in place to address those risks
- Validate processes and controls via walkthroughs or other means
- Develop and execute test plans
- Evaluate test results and remediate design and/or operating control deficiencies where necessary

Under a focused project management approach, the work needed to comply with Sarbanes-Oxley was completed. A typical company having accomplished this successfully would now have the following areas addressed: basic documentation in place, key controls identified, test plans developed and, most importantly, control issues that needed remediation.

Yet at the end of this first year, though filings and disclosures indicate that compliance has largely been achieved, an examination of the processes that companies are left with should call into question whether current methods are operationally sound—and if future Sarbanes-Oxley compliance can be executed with economic efficiency.

Sustainable Sarbanes-Oxley compliance is a careful mix of economic viability, social responsibility and sound operations.

# Our Perspective
# Make conformity with Sarbanes-Oxley a part of daily business life

We believe that management can use operationally sound methods to cost-effectively address Sarbanes-Oxley requirements. While it may have been necessary to approach first-year requirements as a project to be managed, a truly sustainable approach will require transitioning to a mode in which compliance is well integrated into a company's daily operations.

Adhering to Sarbanes-Oxley rules and regulations must continue, but under a sound, embedded operating structure in which the incremental cost is in line with other operational costs. Designing, implementing and operating such a structure will create new demands for most organizations; the good news is that the level of effort required should be far less than the initial experience.

# Aligning annual and quarterly reporting

A sustainable compliance process that deals with Section 404 should benefit management's requirements with regard to Section 302. Therefore, the support needed to align quarterly reporting under Section 302 with annual reporting under Section 404 constitutes a primary challenge for management.

Prior to the completion of first-year Section 404 compliance, many companies used a cascading representation letter for the purpose of confirming the effectiveness of and identifying changes in Disclosure Controls & Procedures (DC&P). These representation letters allowed operational and financial management to confirm that all important issues had been identified and communicated for disclosure in the company's quarterly reporting.

The Securities and Exchange Commission has noted that internal control over financial reporting, in many instances, is considered a subset of DC&P. And, as a result of having just completed an assessment of internal control over financial reporting, some companies have now questioned whether their representation letter approach is adequate. A common concern among executives is how to establish a mechanism that both confirms the evaluation of DC&P on a quarterly basis to support the Section 302 certification, and provides for the periodic testing of controls over financial reporting for the annual Section 404 assertion. Given the level of regulatory oversight, this is a decision that should not be taken lightly.

Under Section 404, management demonstrates through testing that internal controls over financial reporting operate effectively as of year-end. Under Section 302, management certifies that it has evaluated its DC&P as of quarter-end. Section 302 also requires management to report material changes to its internal control over financial reporting. This includes changes resulting from overt business actions taken by management, as well as changes resulting from a degradation of controls over time.

We see companies considering several alternatives. Although testing is not specifically prescribed in order to comply with the requirements of Section 302, some companies are executing test plans throughout the year, allowing for timely recognition of control issues, remediation and retesting, if needed, as well as for the updating of the control evaluation at year-end. Through testing, management attains comfort with regard to quarterly reporting, while at the same time accomplishing the work required for the year-end assertion.

Other companies may choose to perform tests quarterly for what they consider to be higher-risk processes and controls, supplemented by self-assessments for other processes. A third possibility is to rely solely on a self-assessment process for quarterly reporting, with no reliance on testing for the evaluation of DC&P. Complicating consideration of these alternatives are the nature and frequency of the control activities performed, which can dictate the timing and extent of testing.

Choosing from among these alternatives is dependent on management's comfort with the alternatives. Fundamentally, the chosen approach must enable the identification of material changes in internal control over financial reporting and provide reasonable assurance that controls over financial reporting are effective at quarter-end, as well as at the end of each fiscal year.

## Anticipating the impact of change

A second challenge for most companies' ongoing compliance is the ability to recognize and proactively address the impact of change on the organization. Change, whether intended or not, affects the company's business processes and control infrastructure. This, in turn, affects Sarbanes-Oxley documentation and subsequent testing requirements.

The nature of business dynamics will dictate the degree of change companies must deal with in their ongoing program. For major changes, such as system implementations, acquisitions or divestitures, or adoption of new accounting standards, compliance may be implemented as part of the project plan.

Updating or creating process and control documentation and performing testing for the effectiveness of related controls over financial reporting should be considered at the outset of a major change. Indeed, a failure to address Sarbanes-Oxley requirements in the plan for a significant business change has the same impact as a failure to include any major step in the project—more stress later and the potential for delay and cost overrun.

Minor changes also need to be identified and addressed. Employee movement, business process adjustments or technology enhancements are all examples of changes that have the potential to affect compliance.

One approach for identifying changes that could otherwise go unnoticed is for process owners to perform a periodic walkthrough of business processes. Any significant deviation from the documented process is a strong indicator that a business change has occurred. In such cases, documentation and test plans for the evaluation of key control design and operating effectiveness will need to be updated. Self-assessment questionnaires and an annual risk assessment are also useful tools for identifying change.

Addressing the impact of change and the support required for management's reporting responsibilities are not one-time events. Business activity is continuous, and therefore Sarbanes-Oxley compliance needs to be continuous. Companies that do not already have one will need to build a program into the core of their business operations so that changes that impact internal control over financial reporting, no matter how subtle, will be promptly recognized. Management would then monitor ongoing control effectiveness and accommodate, within the overall control design, the impact of change on the organization.

Acknowledging that a reasonable, ongoing program must be developed, the salient question now becomes: how do companies move from project management mode to one of sustainable compliance?

# Building a sustainable Sarbanes-Oxley compliance process

Several elements must be considered in developing a compliance process that is responsible, cost-efficient and effective.

These can be classified into three major categories:

1. An accountability structure that ensures the appropriate level of oversight and process ownership and drives the right attitude throughout the business
2. An operating structure that facilitates cost-effective and streamlined processes for execution of Sarbanes-Oxley requirements
3. A technology support structure that supports the efficiency and effectiveness of compliance processes

## 1. Accountability Structure

The accountability structure needs to define ownership of the design and operation of controls within the organization and create the appropriate tone at the top to reinforce delegation without allowing abdication.

To form a structure that works for the long term, one important task is to define appropriate organizational roles and responsibilities. After this is done, management should communicate what people are supposed to do and reinforce accountability to ensure that they do it.

*Roles and Responsibilities*

Ultimate accountability for adherence to Sarbanes-Oxley rules and regulations, at the enterprise level, rests with the **CEO** and **CFO**. The Board of Directors and Audit Committee need to see that the CEO and CFO have integrated risk and control into the culture of the organization and have appropriately delegated responsibilities to all staff levels in the organization.

Executive responsibility is demonstrated through routine communications that reinforce a control consciousness in the organization; inclusion of internal control reporting on appropriate agendas; and by holding subordinates responsible for control effectiveness related to their respective areas of responsibility. The role of a **Disclosure Committee** is critical to helping fulfill this executive responsibility, as the committee considers and brings to the attention of the CEO and CFO the key issues related to reporting. The Disclosure Committee may further reinforce accountabilities in the organization through its evaluation of such issues.

**Business unit leaders** also have an important role—it is to these individuals that the CEO and CFO will most likely delegate responsibility for assuring the ongoing effectiveness of internal control. Why? Because business unit leaders are responsible for the ongoing operation of all business processes in their respective units, and among the business processes will be those that impact financial reporting.

To fulfill their role in Sarbanes-Oxley compliance, business unit leaders must have a mechanism to assure that control processes under their domain operate as intended. Creating this mechanism will require a new understanding of the elements of control and financial reporting.

**Internal Audit** has generally played a significant role in the first-year effort, a role that now needs to be carefully considered. Traditionally, Internal Audit has been responsible for the oversight and monitoring of compliance with both operational and financial policies and procedures. It has also had oversight responsibility for other compliance programs. Moreover, Internal Audit's role in monitoring these policies and programs is a critical element of management's overall risk-monitoring efforts.

But, according to a PricewaterhouseCoopers survey[1] conducted in November 2004, nearly 60% of the Internal Audit respondents noted that they had dedicated 50% or more of their resources to support Sarbanes-Oxley efforts. Here is one instance in which the question of ongoing compliance can be troublesome: if Internal Audit continues to be relied upon so heavily, this responsibility will likely detract from the department's main function of monitoring all financial, operational and compliance processes and programs.

1 PricewaterhouseCoopers LLP conducted an Internal Audit Alert Internet Survey that closed on November 2, 2004, in which 247 companies subject to the requirements of Sarbanes-Oxley participated.



Has management considered the cost of losing Internal Audit in this traditional capacity? We believe that Internal Audit should be considered an essential part of management's overall monitoring program and should therefore serve as a quality assurance function that will challenge the effectiveness of the company's Sarbanes-Oxley program. This will mean, of course, that responsibilities for day-to-day activities—including testing and business-change documentation—may need to fall to another function within the business.

A growing trend among organizations is the creation of a **Chief Internal Control Officer (CICO)** position. This position can be rolled into that of an existing Chief Compliance Officer or other position of similar nature. It is held by an individual who has taken charge of facilitating and owning the Sarbanes-Oxley compliance process.

While business or process owners own the controls, the CICO provides fundamental guidance and standards for ensuring that actions taken by process owners are adequate to support the year-end management assertion. The CICO is someone who, for the purpose of reporting, captures all testing exceptions and applies consistent guidelines to evaluate the nature of deficiencies. As part of this responsibility, the CICO also monitors remediation activities.

A core responsibility of the CICO is to be the focal point for the identification and evaluation of change. He or she may facilitate the comprehensive risk assessment process—allowing business risk to be analyzed and ensuring that the company can conform to Sarbanes-Oxley requirements even as business changes are implemented. Monitoring testing results allows the CICO to recognize when subtle business changes have degraded existing control activities, an essential step in the timely determination and implementation of proper remediation.

In many companies, the position of CICO reports directly to the CFO with an indirect reporting line to the CEO, Board and Audit Committee. The CICO's activities are validated by Internal Audit.

While business unit leaders are responsible for carrying out Sarbanes-Oxley activities, process owners within business units have influence over the direction of operational and financial processes. **Process owners** should identify change and own documentation and testing of key controls.

Companies should consider including **risk and control specialists** who would likely report to the CICO but be deployed within business units to support both process owners and business unit leaders. There, they would provide hands-on guidance and assistance with updating process and control documentation, developing and executing test plans and evaluating results.

Finally, there are the **employees** involved in business processes impacting financial reporting. As many companies learned in the initial Sarbanes-Oxley effort, involved employees include both operational and financial personnel who need to be trained, and their activities monitored, to ensure the effectiveness of internal controls.

The role of employees in maintaining effective internal control over financial reporting should not be overlooked, especially when, as many businesses discovered during the first year, the majority of key controls over financial reporting are manual.

With the goal of making the Sarbanes-Oxley program a part of the normal course of business, companies should seek to align the organization in such a way that business unit leaders and process owners own documentation and evaluate controls over financial reporting, while Internal Audit acts as a quality control mechanism. The CICO provides standards, practices and support to facilitate the overall execution of the sustainable Sarbanes-Oxley process.

*Communication and Reinforcement of Accountability*

Once the accountability structure is established, the next steps are to communicate and reinforce the roles and responsibilities:

- **Communicate accountability:** Create, update and share with employees relevant job descriptions that include Sarbanes-Oxley roles and responsibilities. Charters of the involved committees should be revised and approved to incorporate details about compliance accountabilities. To further emphasize the importance of an effective internal control environment, organizations should consider including "internal control" as a standing agenda item for the Audit Committee, as well as for business unit operational and financial review meetings.
- **Reinforce accountability:** It is human nature to act on what is measured. Therefore, companies need to develop performance measurements that are in line with the monitoring of Sarbanes-Oxley compliance activities. These can include timeliness measures related to documentation, testing, remediation, etc., as well as operational statistics related to the results of ongoing control-testing programs. A disciplined and routine testing and reporting process will serve to reinforce accountability—ensuring the timeliness of progress and the immediate escalation of issues for evaluation and remediation.

## 2. Operating Structure

The annual assessment of internal control (Section 404) and quarterly evaluations under Section 302 provide valuable mechanisms to ensure that effective internal control over financial reporting is maintained throughout the year. These are not just compliance considerations. Effective control reduces surprises and rework. It decreases inefficiencies, minimizes mistakes and allows management to focus on the future, thus contributing to the overall effectiveness of the company's operations.

*Documentation*

In order to avoid the level of effort expended in the first year, documentation of significant processes, systems and related control activities must be updated regularly. The identification of change will necessitate the creation or updating of documentation. How the documentation effort is triggered will be dependent on the type of change and how the change is recognized—for example, the driver might be a major business change identified through a robust risk assessment process, or a subtle change discovered by a walkthrough or the evaluation of control testing exceptions.

The CICO should prescribe standardized documentation methods (e.g., flowcharts, narratives, control matrices) as well as guidance related to the level of detail to be included. Standardized methods benefit the organization in terms of consistency and ease of review by process owners, auditors and regulators, and encourage a best-practices approach to compliance documentation, including the elimination of excessive levels of documentation.

*Testing Protocols*

Test plans established in the first year, if designed appropriately, would generally remain relevant as long as the controls they are designed to test do not change. Realistically, however, business change occurs continuously—and change is likely to result in new processes. Therefore, standards are needed for the ongoing development and approval of test plans. The office of the CICO is an appropriate authority to establish those standards and review the suitability of test procedures.

A question remains as to who will execute the testing. In the first year, while in project mode, many companies either relied on Internal Audit to execute test plans or turned to outside advisors and consultants for support. Neither of these two alternatives is particularly attractive for the long term, being expensive in out-of-pocket as well as lost-opportunity costs.

Internal Audit's focus on Sarbanes-Oxley testing reduces its ability to help management uncover and resolve other operational and compliance issues. Using external resources on a continuing basis is not only an expensive choice, but one that eliminates the opportunity for employees to use testing as a process to learn the business.

Some companies are addressing the problem by identifying a select group of objective departmental employees who can be trained to conduct the necessary periodic testing programs. This approach has the potential to be less costly over time than relying on third parties for testing, and allows management to demonstrate confidence in employees. For the employees involved, testing provides an opportunity to gain greater knowledge of the organization and exposure to senior business unit leaders and process owners. Such testing is, of course, subject to challenge and oversight by Internal Audit.

Periodic testing is a valuable tool, not just for compliance but also as an effective means to reinforce operating principles that employees are expected to follow. It can be used to identify situations in which employees require hands-on training in control responsibilities due to job changes, program changes, and so on.

Options for testing and evaluating controls throughout the year are many and varied. Therefore, management should carefully consider alternatives, seek guidance internally, propose a course of action and discuss its choice with the company's external auditor. Such actions will ensure that whatever course is selected supports the final evaluation conclusion at each year-end.

*Exception Resolution and Remediation*

Reviewing test results and taking appropriate actions are important components of a sustainable compliance program. A critical success factor will be a timely and quality-driven exception resolution process, in which test exceptions as well as concerns highlighted by self-assessments or other means are evaluated by competent, objective individuals.

The office of the CICO is a prime candidate for undertaking such reviews, having set protocols in place to consistently evaluate and fully understand deficiencies. This is particularly important in evaluating the magnitude and likelihood of potential misstatement to the financial statements.

Identifying where deficiencies overlap also allows the CICO to work with process owners to establish the most efficient approach to remediation. The CICO can centrally monitor and manage remediation progress and provide oversight of retesting procedures. Through this process, issues are flagged and remediation established in a timely manner—a crucial factor in management's ability to carefully consider the implications for both quarter-end and year-end reporting.

*Reporting and Monitoring*

By communicating evaluation and documentation standards, analyzing business risk assessments and monitoring test results, the CICO stays closely attuned to the company's control effectiveness and therefore to Sarbanes-Oxley compliance.

Under this structure, Internal Audit acts as the quality assurance team, providing additional comfort that compliance is being achieved. The CICO captures performance measurements, prepares relevant analyses and, because of the established reporting relationship, shares this information on demand with senior executives, the Audit Committee and the Board. Such a structure allows the individuals who are accountable to be kept apprised of the company's testing and evaluation results, thus contributing significantly to the overall effectiveness of the internal control system.



*Training*

Over the past two years, companies have developed various training programs on Sarbanes-Oxley and internal control. To keep pace with potential modifications and revisions to both the regulation and the interpretative guidance that follows, the CICO needs to develop new training programs and modify existing ones. Each program then needs to be integrated with other employee training.

Tailoring training programs to an audience is the surest way to get results, but when it comes to compliance training, the correct accountability structure must first be in place. Once accountabilities are understood and accepted, training can reinforce them effectively.

Remembering that skilled, competent and objective personnel are required to perform testing, a robust skills-training program should be on every company's priority list for ongoing compliance. This program typically includes:

- Periodic workshops for the Board, Audit Committee, Disclosure Committee and other responsible parties
- Sarbanes-Oxley training as part of new-hire orientation
- Certification training for process owners or risk and control specialists in internal control

Mandated training sends a very clear message that upholding the effectiveness of internal control is imperative.

While some training programs can be very technical, a well-rounded training program should also include seminars on the sharing of best practices in the business—from optimal control design to streamlining and standardizing of financial and operational processes. This is an opportunity for business units to learn from one another and for the business to benefit from the collective understanding and ideas of its employees.

### 3. Technology Support Structure

A significant issue emerging from first year Sarbanes-Oxley efforts is the ineffective use of technology. Going forward, the CICO must involve the IT department in proactively identifying opportunities—based on clearly defined compliance processes—to leverage technology, both to improve controls and to enable an effective Sarbanes-Oxley program.

Using technology to automate controls and manage the compliance process enables:

- Improvement in the quality of information and speed of delivery
- Assurance that compliance steps (e.g., testing) are performed in accordance with the program design
- Identification and management of events in a consistent and auditable manner
- Accountability in the management and reporting of events through a "closed loop" environment

These results lessen the effort required to comply with Sarbanes-Oxley, speed the identification of problems and reduce the amount of rework needed.

No single technology solution achieves all of these benefits. Instead, companies will want to combine several types of functionality—some of which are available in their current technology environment and others that they will acquire. These include:

- A company's core processing systems (such as their ERP and HR systems)
- Enhancement of controls around the core processing systems (such as tools that help with segregation of duties and process integrity)
- A company's core IT infrastructure (such as tools that help with user access, identity management and monitoring IT change management)
- Data integration capabilities (such as databases and XBRL and web services)
- Process automation and monitoring systems (such as business process management platforms)
- Compliance reporting tools (such as business intelligence and corporate reporting platforms)
- Compliance management tools (such as incident, learning or document management and work flow systems)

By developing a technology architecture that pulls together data from disparate systems and uses appropriate functionality to enforce accountability, improve data quality and identify incidents, companies can bring compliance to life for a fraction of the cost of implementing other business applications.

Some companies will want to acquire a compliance management tool. The starting point in selecting this piece of enabling technology is understanding the company's compliance framework (i.e., its accountability structure and operating structure) and then identifying information flows to facilitate it. Considerations include functionality needed in the short term and functionality preferred as the compliance processes mature—workflow, facilitating communications, reporting dashboards, sorting, version control, file size, storage, archiving, etc.

For example, the Sarbanes-Oxley program will likely need a place to house process documentation as well as templates used to assess the design effectiveness of controls within each process. This system needs to be accessible by internal and external auditors as well as by process owners when business changes require updating process documentation, and it needs to house test plans and test results.

Functionality should also support the communication of testing requirements, summaries of test results and a sorting process to quickly separate areas that are passing the tests from those that are not. Built-in reporting to business unit leadership of testing exceptions accelerates the process of remediation. Some technologies today can also provide a basis to extract and analyze business information and metrics from underlying systems for early warning of control problems.

Before choosing from among many tools in the marketplace, a company should review its broader risk and compliance technology needs, considering how those needs are managed. This may reveal an existing technology base that can be adapted to support the Sarbanes-Oxley program. In addition, the review may identify other compliance needs that could be addressed simultaneously.

To enable technology effectively, the task at hand is to: 1) engage the IT department in proactively identifying opportunities to leverage technology in the control environment as well as in the compliance process, 2) define a technology architecture, 3) identify components to be acquired, and 4) lay out a phased approach to implementation. These steps enable repurposing existing functionality and selectively acquiring new capabilities to support a sustainable Sarbanes-Oxley program.

# Enhancing internal control

Meeting the requirements of Sarbanes-Oxley Section 404 can be an expensive endeavor if the underlying control environment is complex, inadequately automated, characterized by duplication in controls and largely reliant on detective rather than preventive controls. Yet this is precisely the state in which most companies found their controls when they began their Section 404 preparations. Much progress has been made, but for many companies cost-effective compliance requires the continued streamlining and automating of controls.

Companies should also seriously consider revisiting actions taken during the first year to remediate deficient key controls. Time constraints forced many companies to undertake temporary and inefficient remediation activities in order to pass the year-end test—leaving a remediation process characterized by labor-intensive manual reviews.

For many companies, cost-effective compliance requires the continued streamlining and automating of controls.

Action is needed to readdress remediation and enhance controls over financial reporting. Steps to be taken include:

- Evaluating the root cause of the control failure
- Addressing the end-to-end process to ensure that solutions do not negatively affect up- and down-stream processes
- Eliminating duplicate controls and replacing detective controls with preventive controls
- Automating controls to eliminate slower, error-prone manual processes
- Improving the underlying business processes

Responsibility for these actions lies squarely with the business units and process owners. The CICO should encourage process owners to identify inefficiencies and plan improvements in the control environment.

# Implications
## Sustainable compliance requires a focused, defined program

The first year of Sarbanes-Oxley compliance has given companies unexpected insight into their operations. Many now see a great opportunity to streamline, standardize and simplify inefficient business processes—an effort that brings its own intrinsic benefit to the company and forms the foundation for a more cost-effective compliance environment.

Now is the time to absorb first-year lessons and make conformity with Sarbanes-Oxley a part of daily business life. Embedding it in the business provides an optimum approach to sustainability and will foster the culture needed to comply with Sections 302 and 404 on a continuing basis. It is the antithesis of an event-driven approach, and one that will require a focused, defined program designed to operate year after year as a natural component of the business.

We believe that companies should begin now to find their own path to sustainable compliance.

# How to build a sustainable Sarbanes-Oxley compliance process

We believe a sustainable environment relies on three key structural elements: organization, operations and technology.

01

## How to establish an organizational structure with clear accountability

Establish clear responsibilities of the Board, Audit Committee, senior management and business unit leaders to reinforce control consciousness and enforce accountability.

Place active oversight of and development of standards for Sarbanes-Oxley compliance in a Chief Internal Control Officer or similar position.

Count on business unit leaders and process owners to identify change, own documentation and testing, and recommend key controls for testing or self-assessment.

Put risk & control specialists in the business to support process owners and business unit leaders with guidance and hands-on assistance.

Place Internal Audit in a quality control role rather than active participant on behalf of management.

Create and update job descriptions, internal control policies, charter, etc., to include details about Sarbanes-Oxley compliance responsibilities.

Develop performance measures aligned with Sarbanes-Oxley compliance activities.

02

## How to create an efficient operating structure

Perform quarterly assessments in order to ensure that effective internal control over financial reporting is maintained throughout the year, and provide management assurance for 302 reporting. Alternative approaches include:

- Executing testing plans throughout the year, allowing for timely control deficiency identification and remediation and retesting
- Performing quarterly testing for higher risk processes and supplementing testing with self-assessments for other processes
- Relying completely on a self-assessment process

Build Sarbanes-Oxley requirements into the project plans for major changes, such as system implementations and acquisitions or divestitures.

Institute processes, such as self-assessments and walkthroughs, to identify minor changes that could affect Sarbanes-Oxley compliance.

Leverage the results of an annual risk assessment to confirm identification of all relevant changes.

Establish standardized documentation methods (e.g., flowcharts, narratives, control matrices) as well as guidance related to the level of detail to be included.

Develop standards for the ongoing development and approval of test plans.

Involve departmental employees in testing to reduce cost and reinforce operating principles that employees are expected to follow.

Develop a timely and quality-driven exception resolution process.

Provide central monitoring and management of remediation progress and the status of retesting.

Capture performance measures, prepare relevant analyses and share information with senior executives, the Disclosure Committee and the Audit Committee and the Board.

Provide comprehensive training tailored to the audience, including:

- Periodic workshops for the Board, Audit Committee, Disclosure Committee and business unit leaders
- New-hire orientation
- Certification of risk and control specialists
- Seminars for sharing of best practices

03

## How to build an enabling technology support structure

Engage the IT department in proactively identifying opportunities to leverage technology, both to improve controls and to enable an effective compliance program.

Define a compliance technology architecture that pulls data from disparate systems and uses them to enforce accountability, improve data quality and identify exceptions.

Leverage existing technology infrastructures to support the compliance process and to improve the control environment.

Review the company's broader risk and compliance requirements to identify other needs that can be met while building a technology base to support Sarbanes-Oxley compliance.

## The Role of the Chief Internal Control Officer

This function can be established anew or rolled into that of an existing Chief Compliance Officer or other similar position. The CICO often reports to the CFO with an indirect reporting line to the CEO, Board and Audit Committee.

The following activities are central to his or her role and are subject to evaluation by Internal Audit on a periodic basis:

Provides fundamental guidance and standards for ensuring that actions taken by process owners are adequate to support the year-end management assertion.

- Prescribes standardized documentation methods (e.g., flowcharts, narratives, control matrices) as well as guidance related to the level of detail to be included
- Establishes standards for ongoing development and approval of test plans and reviews the suitability of test procedures
- Sets protocols to consistently evaluate and fully understand deficiencies

Facilitates the execution of the Sarbanes-Oxley compliance process.

- Acts as focal point for the identification and evaluation of change
- Facilitates the comprehensive risk assessment process
- Analyzes business risk assessments
- Oversees risk and control specialists who are deployed within business units to support both process owners and business unit leaders
- Monitors testing results and recognizes when subtle business changes have degraded existing control activities
- Captures all testing exceptions and applies consistent guidelines to evaluate the nature of deficiencies
- Establishes, with process owners, the most efficient approach to remediation
- Monitors and manages remediation progress and provides oversight of retesting procedures
- Captures performance measurements, prepares relevant analyses and shares this information on demand with senior executives, the Audit Committee and the Board
- Develops and presents tailored training programs for key stakeholders in the organization
- Works with IT to identify and/or leverage technology to manage the compliance process
- Encourages process owners to identify inefficiencies and plan improvements in the control environment

For further information, please visit
www.pwc.com/governance

or call
1.800.639.7576