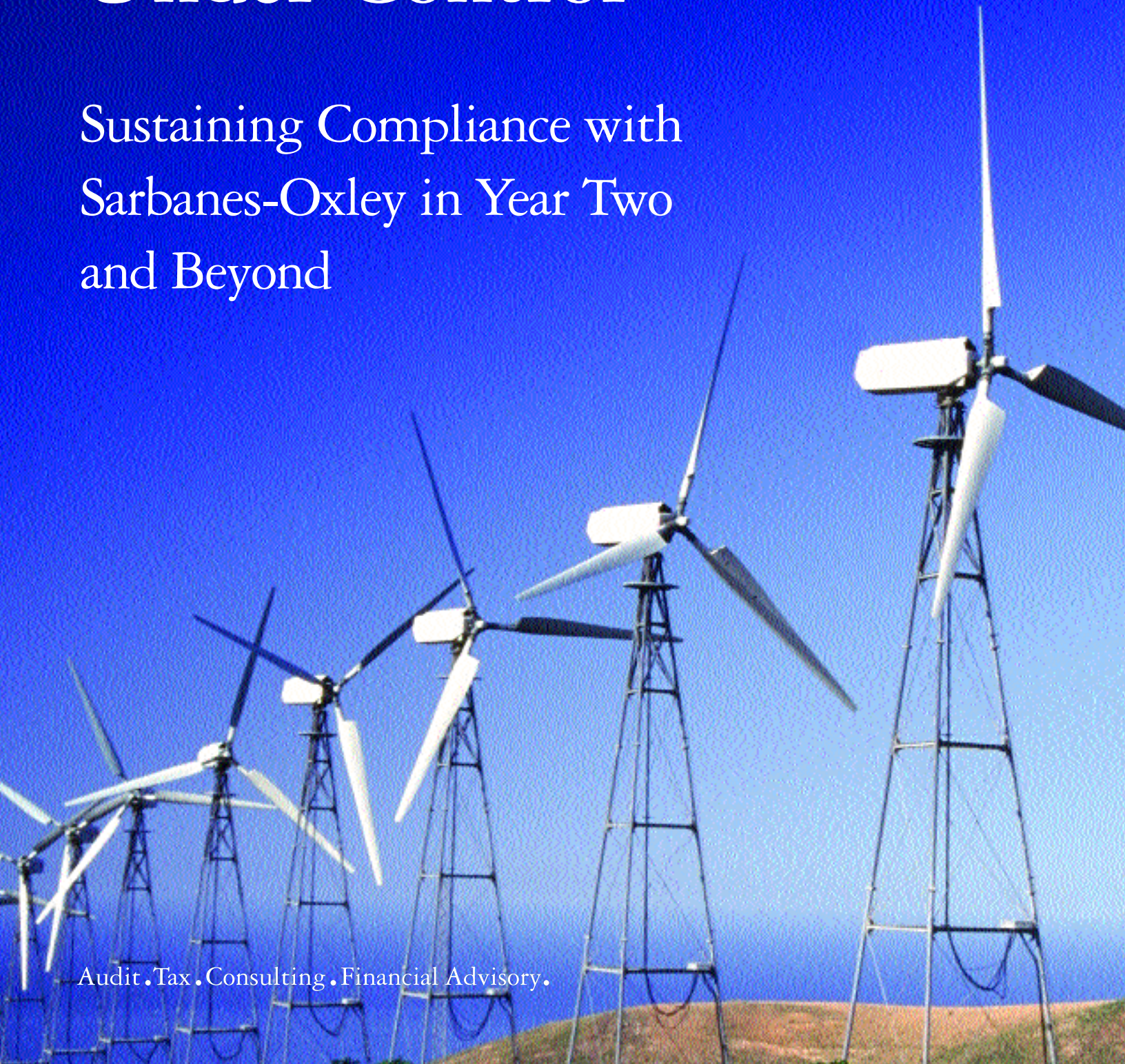
Deloitte.

Under Control

Sustaining Compliance with Sarbanes-Oxley in Year Two and Beyond



Audit . Tax . Consulting . Financial Advisory.

Table of Contents

Under Control

Sustaining Compliance with Sarbanes-Oxley in Year Two and Beyond

SARBANES-OXLEY, ACT I

When Senator Paul Sarbanes and Representative Michael Oxley set out to "fix" corporate disclosure and financial reporting, they sought to quell a volatile situation: corporate scandals arising frequently; market confidence falling rapidly; and an unnerved public clamoring for corrective action.

The lawmakers crafted the Sarbanes-Oxley Act of 2002[1], which pundits quickly hailed as a landmark remedy. Although prior legislation — most notably the Federal Deposit Insurance Corporation Improvement Act and U.S. Federal Sentencing Guidelines — had tackled formidable business issues, Sarbanes-Oxley set precedent in the far-reaching obligations it placed on public companies. As a result, no one — from business, government, media, or academia — could be certain how the law would play out as it evolved from abstract legislation into real-world application.

Among the requirements causing consternation in the business community was section 404 — "Management Assessment of Internal Controls" — which called on public companies to identify financial reporting risks, ascertain related controls, assess their effectiveness, fix any control deficiencies, and then re-test and re-document anew. For companies of all sizes, but especially those with complex organizational structures and far-flung subsidiaries, the task proved daunting. Indeed, so challenging was section 404 implementation that the Securities and Exchange Commission thrice delayed compliance deadlines, once in 2003 and twice during 2004.

Despite the substantial resources — in time, personnel, and dollars — companies expended on compliance, the section 404 work was often difficult and sometimes chaotic.

Today, the first conformance dates have come and gone for many companies. And with results tallied and lessons learned, it appears that the initial trepidation was justified. Both empirical and anecdotal evidence show that despite the substantial resources — in time, personnel, and dollars — companies expended on compliance, the section 404 work was often difficult and sometimes chaotic. Many executives, spent from the exertion, reached the same conclusion: This kind of monumental effort simply can't be sustained in perpetuity.

Fortunately, it doesn't have to be.

[1] For purposes of this document, the terms "Sarbanes-Oxley" and "the Act" refer to the Sarbanes-Oxley Act of 2002 in its entirety, including all sections of the law enacted by Congress, all associated rules promulgated by the Securities and Exchange Commission, and all related standards issued by the Public Company Accounting Oversight Board. The term "section 404" refers specifically to the "Management Assessment of Internal Controls" section of Sarbanes-Oxley and all the rules and standards that fall under that section.

SARBANES-OXLEY, ACT II

Not to say that companies can now relax; quite the contrary. Compliance must be rigorously maintained from now into the foreseeable future. But moving forward, the strenuous labor that led to the first-year finish line needn't be as frantic and all-consuming.

Indeed, a replay of the year one compliance fire drill is as untenable as it is unwise: Few companies could again marshal the resources or survive the disruption. But if year two under Sarbanes-Oxley is to cause less pain and provide more gain, companies must plan, design, and implement an efficient and effective program for sustainable compliance. Anything less will likely result in unacceptably high costs, heightened risk, distraction from the corporate mission, and, ultimately, competitive disadvantage.

Sustainable compliance, on the other hand, may provide long-lasting benefits that transcend the original intent of the Act. A well-designed and intelligently implemented sustainable framework potentially can:

- help reduce the cost of compliance
- optimize controls and related processes
- integrate financial reporting and internal control processes
- streamline management's quarterly and annual certification of financial results and controls
- redirect compliance efforts away from risk aversion and toward risk intelligence
- improve accountability throughout the organization
- enhance market competitiveness

Critical to the success of this conversion from short-term compliance to long-term sustainability will be leveraging all that has been learned. Every company that has met the requirements of section 404 has documented, evaluated, tested, and remediated controls and has gained a better understanding of their operations in the process. The section 404 work has provided valuable knowledge and insights about controls, processes, systems, and organization, and has shed new light on challenges and opportunities for improvement. Thus, these companies are now presented with an occasion to exploit this accumulated knowledge and extract value from their substantial investment in compliance.

(Companies that came up short in their compliance efforts — either by failing to meet the reporting deadline or by uncovering material weaknesses — will obviously have different issues to address.)

In other words, companies that successfully navigated the first year of Sarbanes-Oxley now have the rare opportunity to convert an expense — compliance — into an asset — sustainability.

YEAR ONE IN REVIEW

When astronauts return from space, they are immediately whisked to a debriefing session to capture valuable information while it is still fresh. A similar procedure should be employed for Sarbanes-Oxley efforts.

Among the more notable outcomes of year one was the admirable performance of public companies — as well as some private, nonprofit, and governmental organizations — which distinguished themselves through their commitment and resolve. A large segment of the business community met the challenge of elevating the integrity and reliability of financial reporting and restoring investor confidence. The job is by no means finished, but progress has been substantial.

And progress can be accelerated through a clear-eyed examination of the last year. This includes reviewing and evaluating results of first-year assessment activities; identifying lessons learned and areas requiring improvement; obtaining feedback from the independent auditor and internal audit; and identifying and considering other benefits that may be achieved beyond compliance.

Additional value can be gleaned through a scrutiny of shortcomings. Compliance efforts may have been impeded in the following areas:

1. Project Mindset: With deadlines looming, many companies understandably treated section 404 compliance as a discrete project with a clearly defined ending point.

Employees were borrowed from various departments; internal audit's focus was redirected; consultants were hired; and other business initiatives were postponed while the effort was underway.

But this "project" mindset will prove a hindrance to long-term compliance efforts. There is, of course, no end date for section 404 compliance, any more than there's an end date for 10-K filings. Whether companies are closing the books on the numbers or closing the books on internal control, reporting requirements are rolling and continuous.

Business gurus often use metaphor to describe the proper approach: *Good governance must be stitched into the fabric of the company. Strong internal control should become part of the corporate DNA.*

However one wishes to describe it, the underlying message remains the same: The tenets of good governance and internal control must become integrated into the mission, culture, and daily activities of the company.

2. Overextension of Internal Audit: The internal audit function proved a lifesaver for many companies during year one, providing key personnel for documenting, evaluating, testing, and remediating controls. But a couple of problems can arise with continued reliance: One, the regular tasks of internal audit — operational, systems, and special project audit work — suffer when the function is redeployed. If management continues to utilize internal audit for intensive section 404 and 302 compliance-related work, then a significant infusion of resources (i.e., budget and headcount) to accommodate the additional workload will be needed. And two, if internal audit is placed into the position of concluding on the effectiveness of the controls on behalf of management, then the function may not be considered objective enough to be relied upon by the independent auditors as they determine the extent of testing necessary to support their internal control audit procedures.

3. Poorly Defined Roles: Internal control-related roles and responsibilities, often poorly defined and segregated from the day-to-day routine of employees during the first year, will require greater clarity and integration going forward.

Job descriptions throughout the organization will need revision to reflect new responsibilities. Control responsibilities must be thoroughly incorporated into business routines, a process that may well have a more-pervasive impact on the company than any other change mandated by Sarbanes-Oxley (although that realization has not yet hit many companies).

Section 404 has dramatically increased the responsibilities of the average line manager who engages in activities that feed the financial reports. Just as supervisors may need to manage budgets even though they are not necessarily financial "types," so too must many other employees now address internal control as a core part of their jobs, even though they are not control specialists.

If management continues to utilize internal audit for intensive section 404 and 302 compliance-related work, then a significant infusion of resources (i.e., budget and headcount) to accommodate the additional workload will be needed.

Employees must be held accountable for understanding and performing their proper roles in the post-Sarbanes-Oxley environment. Responsibilities should be explicitly defined, repeatedly communicated, seamlessly integrated, and closely monitored.

Employee education also takes on new significance in sustaining compliance, because allegiance to the creed of internal control and good governance does not magically appear — it must be cultivated. Employees will only embrace the philosophy if they receive proper guidance,

instruction, and modeling. Thus, the slogan of "tone at the top" comes into play. And continuing education on business ethics, internal control, Sarbanes-Oxley, and related topics becomes an ongoing need.

Finally, the first-year practice of redeploying staff to fill Sarbanes-Oxley gaps will, in most cases, prove unworkable over time. Depending on company size, internal control-specific employees may need to be hired.

4. Improvisational Approach: Another symptom of deadline pressure showed up in the jerrybuilt practices that carried many companies through the first year. With few opportunities for high-level planning and little time for weeding out duplication and stripping away inefficiency, makeshift methods were devised to document, evaluate, test, and remediate controls.

Savvy managers will *make* the time for planning and analysis in year two, knowing that redundant processes, controls, and technologies add burdens and costs to the compliance effort.

This improvisational approach yielded a predictable outcome: internal control assessment processes both more risky and less sustainable than might otherwise have been developed.

Thus, savvy managers will *make* the time for planning and analysis in year two, knowing that redundant processes, controls, and technologies add burdens and costs to the compliance effort. The goal is straightforward: Companies must put into place carefully considered, well-designed, repeatable processes.

5. Underestimation of Technology Impacts and Implications: Before most section 404 projects got off the ground, conventional wisdom held that compliance would have little or no impact on information technology (IT). Today, that viewpoint has been discredited. In fact, IT is recognized as critical for achieving the goals of the Act, and the impact and implications of technology are widely regarded as significant and pervasive.

In many year-one projects, organizations focused heavily on business processes and did not consider the broader role that IT plays in managing financial information and enabling controls. Working under deadline pressure and without a prescribed roadmap, executives found it difficult to define the scope of IT's involvement and the assessment of the related controls. As such, the effort involved was underestimated and attempts to address the technology aspects were, in some cases, haphazard. Companies often found the IT component of their overall compliance effort to be informal, inconsistent, and manually intensive.

First-year readiness efforts highlighted disconnects between the IT and finance functions. Alignment between IT and business needs is not a new challenge, but the controls documentation and assessment activity shed new light on the issues. It became clear that IT is critical to efficient and effective controls, and to the production and maintenance of high-quality financial information.

Compliance with section 404 also created the need for technology solutions to support management of the newly required documentation, evaluation, testing, monitoring, and reporting activities. Although software vendors worked diligently to address the issues (and the opportunities) presented by Sarbanes-Oxley section 404, inevitably, a lag developed between customer requirements and product delivery. But technology is catching up to the market needs, and IT will make a huge impact on compliance going forward.

At a minimum, technology investments will be necessary to support sustainable compliance in several areas, including repository, work flow, and audit trail functionality. Technology will also be used to enable the integration of financial and internal control monitoring and reporting — a critical requirement at most large and complex enterprises.

Especially important will be systems that provide executives with a "dashboard" or "portal" view of the status and performance of controls, linked to financial information. This integrated approach will allow users to drill down from financial results to the underlying controls, and automatically flag exceptions, unauthorized entries, and other anomalies. Such solutions exist today in rudimentary forms; however, development will likely proceed at a rapid pace and more sophisticated products will become available. As the focus on technology increases, the benefits to companies will be substantial, including more timely and accurate information regarding controls performance; corroborated data regarding financial reporting and the underlying controls, and overall improved oversight for management and the board.

In most cases, the efficiencies gained by leveraging such technology will rapidly offset the implementation costs. Conversely, the costs and risks of not automating to the fullest extent possible could be significant.

6. Ignored Risks: Effective internal control is predicated on risk. Indeed, what many consider to be the heart of a section 404 compliance effort — the controls themselves — exist expressly for the purpose of minimizing the risk of financial reporting errors.

Yet paradoxically, for some companies in year one, risk assessment was treated as an afterthought — if addressed at all. Companies often failed to develop and deploy a comprehensive risk assessment process as part of their compliance projects, an outcome both surprising — because risk assessment is an inseparable component of the COSO internal control framework — and unfortunate — because without proper risk assessment, much of the time and dollars spent documenting and testing controls may have been squandered.

In the absence of a risk-based approach, companies had no way to prioritize their activities. Some focused on the wrong areas, which resulted in a disproportionate amount of time spent documenting and testing controls that didn't mitigate true risk, i.e., controls that, if they failed, couldn't contribute to a material misstatement.

Which begs the question: If companies haven't undertaken a comprehensive risk assessment process, then how can they design effective procedures to address those risks?

The answer, of course, is they can't!

The solution is to get the cart back behind the horse: Establish a company-wide risk management program — a formal, regular process designed to identify key financial reporting risks, assess their potential impact, and link those risks to specific areas and activities within the organization.

YEAR TWO IN PREVIEW

Most companies that complied with the first-year requirements of section 404 of Sarbanes-Oxley did so at considerable expense and significant effort. To ensure that all the work wasn't for naught, a key objective in year two will be to derive value from that undertaking.

> Sustainability is a cumulative and evolutionary process.

Much of the year-one compliance work — from the controls documentation to the test plans, from risk assessment to communication strategies — can and should be leveraged for the future. Sustainability is a cumulative and evolutionary process; companies should endeavor to build upon their initial gains by developing a holistic internal control plan for the coming year.

The first-year experience also emphasized the point that it is hard to play catch-up. A better tactic is to be proactive: Companies should think about internal control in advance of organizational initiatives, projects, and potential acquisitions.

For example, due diligence conducted before a merger or acquisition should take into consideration the system of

internal control that will be inherited and integrated upon consummation of the deal. Similarly, any information technology upgrade or implementation project should have a strong focus on the internal control aspects from inception.

The objective is clear: Year two efforts should focus on sustainability and forward thinking. The risk is real: Without sustainability, backsliding may be inevitable, and companies may soon fall out of compliance. And thus the question is paramount: How can companies develop a rational, methodical, efficient, and economical approach to the problem of sustainability?

SUSTAINED COMPLIANCE SOLUTION FRAMEWORK

Judging from the frenetic activities of the last year, one might reasonably conclude that Sarbanes-Oxley compliance is the number one goal of public companies. Such a notion is, of course, folly. Compliance, while important, should never be mistaken for the corporate *raison d'être*. Rather, it is a means to an end, a necessary element in the quest for business success.

Compliance, while important, should never be mistaken for the corporate *raison d'être.* Rather, it is a means to an end.

Year two represents an opportunity to put Sarbanes-Oxley compliance back in its proper place, alongside other legislation, rules, regulations, and standards that businesses typically face. One way to accomplish this, paradoxically, is to so fully integrate compliance activities that they become an indistinguishable part of the ongoing business, utilizing a framework that simultaneously reduces cost, complexities, and risk.

To help companies move from a project to a program, Deloitte developed the Sustained Compliance Solution Framework. Among its most notable characteristics, the framework provides for:

- effective and efficient processes for evaluating, testing, remediating, monitoring, and reporting on controls
- integrated financial and internal control processes
- technology to enable compliance
- clearly articulated roles and responsibilities and assigned accountability
- education and training to reinforce the "control environment"
- adaptability and flexibility to respond to organizational and regulatory change

Three interlocking components drive the Sustained Compliance Solution Framework: people, process, and technology.

PEOPLE

The "people" component of the Sustained Compliance Solution Framework refers, as one might expect, to the human resources and organizational elements necessary to sustain compliance. Tasks required to get people in line include the following:

Formalize the compliance and governance structure
Most companies have already drawn up a working blueprint for this, and may only need to make some minor corrections. Activities include forming committees (steering, disclosure), teams (internal control), offices (program management), and other organizational structures.

Define roles and responsibilities
The more deeply the philosophy of strong internal control is imbedded in the corporate culture, the more sustainable compliance becomes. Thus, every job function that has any impact on or relation to financial reporting (and there are many more than one might initially expect) may need to have its job description updated to include internal control responsibilities.

Companies may also have to consider creating new jobs, such as internal control specialists, and even establishing entirely new groups or divisions to assume responsibility for internal control.

When defining appropriate roles related to section 302 and 404 compliance, it's important to keep this fact top of mind: Management is explicitly and solely responsible for internal control. No other party can fill this role.

However, that shouldn't lead one to conclude that top executives need to do all the work themselves. In fact, they can and should leverage all the resources within and outside the organization necessary to get the job done.

Define the role of internal audit

Notable among the resources cited above is internal audit, which should play a significant role in any compliance program. As cited previously, internal audit proved indispensable in the first-year compliance efforts at many companies. In a survey of Deloitte clients, internal audit led the Sarbanes-Oxley section 404 project outright at more than half the companies. In more than 80 percent of the cases, internal audit was providing all or some of the resources. And rightfully so. After all, who else in the company is more knowledgeable about internal control and better versed in developing a testing methodology?

The skills and resources that internal audit brought to the table in year one can be drawn upon again going forward, with the one caveat described previously: If internal audit is going to be called upon to provide its resources, then the function's budget should be revised upwardly to reflect these new responsibilities. Unlike year one, where internal audit was often redeployed at the expense of other duties, going forward the function should grow to encompass both its traditional and new roles.

What, precisely, should this new role be? Recent guidance from the Institute of Internal Auditors suggests that appropriate roles for internal audit include the following[2]:

- support management and process owner training on project and risk and control awareness
- perform quality assurance review of process documentation and key controls before hand off to the independent auditor
- advise management regarding the design, scope, and frequency of tests to be performed
- be an independent assessor of management testing and assessment processes
- perform effectiveness testing to support management's assertions
- aid in identifying control deficiencies and review management plans for correcting the same
- perform follow-up reviews to ascertain whether control deficiencies have been adequately addressed

Certain tasks, however, should remain under the purview of management. The IIA contends that management should assume direct responsibility for:

- setting the risk appetite
- creating risk management processes
- performing risk assurance
- making risk response decisions and taking action on them

Management is explicitly and solely responsible for internal control. No other party can fill this role.

Attaining the proper balance of responsibilities is critical. If a single team — be it internal audit or management — performs all of the tasks required to assert to the effectiveness of internal control, then the independent auditors would rightfully conclude that the testing process lacks sufficient objectivity, because those who were responsible for the controls would also be testing the controls. This situation would result in the independent auditor having to perform all effectiveness testing for purposes of supporting their audit procedures. But dividing responsibilities as outlined above will allow the independent auditors to rely on the testing work to the fullest extent possible, thus improving the efficiency and timeliness of their work.

[2] Institute of Internal Auditors, "Internal Auditing's Role in Sections 302 and 404 of the Sarbanes-Oxley Act," 2004. Download available at http://www.theiia.org/iia/download.cfm?file=1655

Identify needed skills and competencies
As most companies learned over the past year, internal control is a highly specialized subject requiring detailed knowledge, sophisticated judgment, and a multitude of skills (e.g., people skills and technical skills). Those staff that are dedicated full-time to internal control should be properly trained in the required skill-sets. Companies should consider incorporating employees into a career development model similar to those of other finance and internal audit jobs.

Create a staff development strategy and supporting plans
If recruiting difficulties, corporate philosophy, budget constraints, or other factors lead a company to keep its talent search in-house, a strategy must be developed to ensure staff competency. Budget allocations, personnel deployment, education and training, and other considerations will require attention.

Keep employee training programs robust and up-to-date
Under a strong system of internal control, employees are armed with all the tools and information they need to respond to change.

No system of internal control, however well planned, will be failsafe from the outset. And no person or team will perform error-free, especially in the early years of compliance. The key is not so much preventing errors as it is recognizing and responding to them. A watchful eye should be maintained for patterns of control deficiencies, which may indicate an area for additional training.

External factors can also impact compliance. Any piece of legislation as complex as the Sarbanes-Oxley Act will be subject to frequent change, not necessarily to the Act itself, but rather to the rules and standards that evolve from the law. Thus, it is critical to monitor the guidance that is periodically issued by the Securities and Exchange Commission and the Public Company Accounting Oversight Board, and augment employee education programs as required.

Training that is responsive to changing conditions — both internal and external — can take many forms. For example, individuals who are responsible for internal control testing may need training on methodology, sample sizes, and control deficiency evaluation. Board and audit committee members could require guidance on the nuances of internal control, financial analysis, oversight responsibilities, and expectations and limitations. Senior management may benefit from instruction on evaluating, classifying, and responding to control deficiencies. Internal audit might require education on its new role in the sustained compliance infrastructure. Information technology personnel may need tutoring on the relationship between IT and financial reporting.

Enhance communications
Frequent and open communication is critical to any system of internal control. Communication, both vertically (from boardroom to mailroom) and horizontally (to all geographical locations), is key to setting the ethical tone of the organization and maintaining a strong control environment.

As companies pursue sustained compliance, formal and informal communication channels will help create an environment where business objectives, codes of conduct, and related information can be conveyed consistently throughout the company. Using both broad and targeted messages promotes commonality in expectations, knowledge, and practice. The result is an employee population with a strong understanding of the organization's goals and standards, which will enable them to guide their own activities and behaviors.

Ensure knowledge management and capability transfer
Institutional knowledge that resides only in an employee's head is knowledge at risk. Every facet of internal control should be thoroughly documented and accessible to qualified employees. Especially important are employee operational manuals, which can guide new or temporary personnel who are assuming or filling in roles.

PROCESS

Routine is often a precursor to reliability and sustainability. To create a strong and sustainable system of internal control, reliable and methodical processes are key. The benefits of routine can be many; while the drawbacks of disorder can be substantial. Here are some important elements of success:

Engineer processes
During year one compliance work, some companies developed ad hoc processes; others had no processes whatsoever. Year two is the time to put formal structures in place. Companies should develop and document the particulars around risk assessment, testing, remediation, concluding, and reporting. Certain questions require attention: Who will conduct the work? Under whose supervision? During what timeframe? How does this work flow through to support quarterly and annual reporting requirements?

In designing a sustainable compliance program, it is important to remember that management is responsible for maintaining an effective internal control program 365 days a year. As such, the process engineering should look beyond the quarterly and annual milestones, which, while important, represent only part of the effort. What activities and processes must be accomplished routinely to ensure the effectiveness of the internal control program? What are the day-to-day work elements that make up the program? How should existing processes be revised to support sustainable compliance?

Integrate internal control and financial reporting
Pre-Sarbanes-Oxley, many executives did not take into account the full life-cycle of financial reporting. Instead, they concerned themselves with the numbers found at the final stage of the process — those contained in the financial statements.

With the passage of the law, however, company leaders must now personally certify to the accuracy of the financials, as well as to the related controls, each quarter. This requirement gives them a strong incentive to familiarize themselves not just with the final numbers, but also with the origin and evolution of those figures. As a result, executives are rediscovering that, like the proverbial iceberg, a company's financial reports represent just a small part of the overall picture. What lurks below the waterline — i.e., the processes and controls underlying the numbers — demands careful attention.

Executives are rediscovering that, like the proverbial iceberg, a company's financial reports represent just a small part of the overall picture.

Or, to put it another way, many executives are learning (or re-learning) that internal control and financial reporting are inextricably linked. They are also realizing: the stronger the link, the more reliable the financials.

Strengthening this link should become an important objective in year two. During the first year of the Sarbanes-Oxley era, many companies focused on documenting, evaluating, and testing controls, but often didn't have the luxury of time to address the underlying financial reporting processes. Today, as companies seek to enhance their controls during the move from compliance to sustainability, they should simultaneously work to enhance the underlying financial reporting processes as well — to strengthen the link. This can be accomplished in a number of different internal control areas, including monitoring, reporting, and governance.

From a monitoring perspective, companies should combine the monitoring of financial information and the related controls, in order to provide management with the intelligence it needs to conduct their certifications. To do

so, management should define the information it needs, specify when it is needed, and develop processes that allow management to review control performance concurrently with the review of financial results.

From a reporting perspective, in the first-year frenzy, many companies developed internal control reporting processes that were not integrated with their existing financial reporting processes. As companies seek to develop a sustainable model, the reporting of internal control should be integrated with financial reporting. The processes that feed 10-Q and 10-K filings should be closely linked to those that supply the information for section 302 and section 404 filings.

From a governance perspective, the audit committee is responsible for the oversight of financial reporting and internal control. Therefore, going forward, the audit committee should focus, in addition to financial reports, on internal control and risk management.

While change is often a barometer of success, it can also be a harbinger of internal control headaches.

Manage internal and external change

If a company isn't changing, it probably isn't thriving. New products, expanded markets, shifting priorities, growing revenues, all of these and more are indicators of a dynamic organization. But while change is often a barometer of success, it can also be a harbinger of internal control headaches.

In this new era, virtually every change that a company undergoes will have an impact on internal control. Obviously, major events like a merger or acquisition or a new IT implementation will present significant compliance implications. But smaller, everyday occurrences — personnel moves, department restructurings, market shifts, IT system changes, process changes — will also have a ripple effect. Other external factors — such as new accounting and reporting standards — and internal situations — such as risk of fraud — can have significant implications for effective internal control.

Change happens. And as a result of this natural and continuous evolution, many of the processes and procedures that were so painstakingly documented over the last year will be revised, redundant, or retired over time as the company advances and grows. Additionally, many of the conditions and circumstances that existed initially will have altered. Will this cycle of change repeatedly throw companies back to square one in terms of Sarbanes-Oxley compliance? Or will they have the adaptability and flexibility to respond to organizational, regulatory, and market changes as they occur?

Astute executives will strive for the latter, because managing change is not just a good idea — it's a legal requirement. Under section 302 of the Act, companies must identify and evaluate any material changes to internal control over financial reporting every quarter.

Address risk

So how do managers get their arms around change? The best way to identify and address change is through a comprehensive risk assessment process. Companies should assess risk at least quarterly to meet the requirements of section 302, as well as to keep the organization's financial reporting risk profile in line with the evolution of the business. This assessment should be especially aggressive and thorough during the early quarters of the year, which will allow the company sufficient time to make appropriate changes before year-end.

In addition, companies should re-evaluate their financial reporting risk profile every time they undergo a significant business event. This helps management guard against unpleasant surprises at year-end, when overlooked risks can loom large in an independent auditor's section 404 internal control audit.

Of course, it's a risky world out there, and one might easily get bogged down in the magnitude of the task. But the goal is not to produce a laundry list of all conceivable risks,

but to identify and prioritize risks in the context of the company's unique characteristics and operating environment.

Develop efficient and reliable testing
Applying the most appropriate tests to internal control can be vexing. Self-assessment may be more appropriate for one situation; a dedicated control group for another. Making the proper choices requires knowledge and guidance.

Another variable concerns the use of manual controls vs. automated controls. The latter may be less prone to error or manipulation, as well as impervious to fatigue, distraction, absenteeism, and associated problems.

Further complicating the situation is the issue of testing frequency. Unfortunately, few hard-and-fast rules exist. There are no specific standards for the number of selections nor the types of tests to be conducted. Factors such as the role of the tester, the nature of the control, and the frequency of the control's use will all come into play. Controls that are executed infrequently (annually or quarterly) may require a limited number of transactions to test. Controls in frequent use may require dozens of selections to verify their effectiveness.

Making these determinations is not a simple matter; expertise is required to ensure that the proper tests are deployed and utilized at the appropriate intervals. Internal audit, independent auditors, consultants, and other parties may help in this determination.

Of course, all these issues were dealt with to some degree in year one. Going forward, companies should work for refinement in this area. Equally important, efforts should be made to evenly spread testing activities throughout the year to normalize the workload. Actually, a slight imbalance, with the testing schedule skewed toward the first half of the year, can yield two important benefits: one, early testing can help avoid a year-end crunch; and two, it can provide enough time for control remediation and retesting should any control deficiencies be uncovered.

Take action based on test results
Testing is, of course, important. But its value is diminished unless processes are in place to act upon the test results.

Some testing will yield positive outcomes, which should be duly noted and filed. More important, perhaps, are the procedures for prioritizing and reporting control deficiencies. For this, companies need both a control deficiency governance process and a corporate-level function responsible for gathering, evaluating, and concluding on control deficiencies.

It should be noted that testing activities may not be the only means of identifying control deficiencies. Other avenues may include findings by internal audit, the independent auditor's management letter comments, anonymous reporting through a whistleblower hotline, and other sources.

There are many benefits associated with a control deficiency governance process, and an equal or greater number of risks associated with not creating one. On the plus side of the ledger:

- Companies are able to maintain consistency in the evaluation and resolution of control deficiencies because a central group — with clearly defined roles and responsibilities — assumes responsibility for the process.
- A well-defined process helps demonstrate to independent auditors that the company has an effective internal control assessment process.
- Since the group responsible for evaluating control deficiencies will report directly to management and the audit committee, the magnitude and number of control deficiencies should be transparent to senior management.
- A good control deficiency governance process demonstrates a strong tone at the top, which is a core element of an effective control environment.
- With a clear process and articulated roles and responsibilities, the control deficiency governance process will be an integral component of the company's infrastructure for sustained compliance.

Develop a remediation action plan
The negative ramifications of a control deficiency that is allowed to fester could be considerable, from a market, regulatory, and public relations standpoint. Furthermore, a significant deficiency that is not corrected may be constituted in future audits as a material weakness, since the failure to correct demonstrates a weak control environment.

To avoid such outcomes, a well-defined process should be established for addressing and disclosing internal control issues. This process should specify the critical elements (i.e., the who, what, where, when, and why) of the issue and must be rigorous in its execution, monitoring, and enforcement. As part of this process, companies should make sure they have a procedure for communicating findings to the audit committee.

Design a documentation program
When it comes to documentation, corners cannot be cut. Independent auditors will examine the recordkeeping; internal personnel will draw upon it; in extreme cases, regulators may wish to inspect it. From scoping and planning to execution and implementation — all this and more must be committed to record.

But keeping detailed records is only the start. Attaining the proper level of documentation and maintaining it as a common standard throughout the organization may prove a greater challenge.

Like many other aspects of section 404 compliance, documentation cannot be done and forgotten. Virtually every piece of documentation will have a shelf-life and must be refreshed over time.

Enhance quality
Companies should apply quality improvement processes and approaches to their internal control program with a goal toward constant refinement and ongoing improvements. Best practices should be shared within and outside the organization. The message of quality should be constantly reinforced.

TECHNOLOGY

Knowledgably deployed and utilized, technology can provide the margin of difference between compliance success and failure, especially in large and complex enterprises. In most cases, the efficiencies gained by leveraging technology will rapidly offset the implementation costs. Conversely, the costs and risks of not automating to the fullest extent possible could be significant.

Here are a few steps to make the most out of technology:

Review IT strategy and architecture
As noted above, the rush to finish first-year readiness and testing left little time to step back and fully assess the potential impact and implications of information technology. For year two and beyond, developing a comprehensive assessment of what sustainable compliance means to the IT function, IT business processes and, of course, the IT architecture will be a critical step. A piecemeal approach risks missing important elements.

As the process elements of the sustainable program are engineered, determine the expectations for technology enablement. It is almost certain that new requirements will be defined. Technology vendors have created a wealth of products that can become part of the solution to the various needs in managing the internal control program and financial reporting processes. A thorough investigation of technology options can help extract the most value out of IT. Starting with a big-picture approach can help frame the optimal role of information technology in a system of internal control.

However one approaches the IT elements of sustainable compliance, three fundamental areas must be addressed:

1. technology for managing internal control documentation, evaluation, testing, monitoring, and reporting

2. technology for integrating the monitoring and reporting of financial information and internal controls

3. processes to operate and manage the IT environment in a manner that sustains the effectiveness (and the evidence of effectiveness) on an ongoing basis

Implement technologies for internal control management
The ongoing management of an effective internal control program will require the use of technology for most companies. Although makeshift methods and interim tools characterized many first-year projects, sustainable compliance will require more than "project tools." Today, a number of software products are available to enable management of the internal control program. The core functionality provide the controls repository, work flow, and audit trail. But this is only the beginning. Sustainable compliance must consider ongoing management needs, such as monitoring needs, the ability to drill down from financial results to the underlying controls information, and other requirements such automatically flagging exceptions, unauthorized entries, and other anomalies.

Implement an internal control management "portal"
Sustaining compliance through the management of internal control and financial reporting requires ongoing monitoring. The integration of financial information and internal control is key to monitoring the effectiveness of the program. Enabling "appropriate-time" monitoring, reporting and analysis capabilities will give management the tools it needs to be confident that the "tone at the top" is truly being executed throughout the organization.

Technology-based solutions, currently in development, will allow for continuous monitoring — often through a Web-based platform — of critical controls and their impact on financial information. Using this technology, executives receive internal control information alongside financial data in a coherent and single view. This approach can enhance communication timeliness and efficiency; provide an early-warning system for executives to respond rapidly to internal control issues; and deliver the reliability, economy, and efficiency that are the hallmarks of technology-based tools.

Establish sustainable controls in IT business processes
IT business processes will be an important area of focus in designing and building a sustainable compliance program. Management of the IT environment must consider the new realities of sustainable compliance. The processes, procedures, and enabling technology for managing applications and the infrastructure must be enhanced to manage the internal control program on an ongoing basis. The integrity of the financial systems must be assured and demonstrable, requiring new considerations in change management and system monitoring. This has significant implications for change management and for implementation of new systems.

Although makeshift methods and interim tools characterized many first-year projects, sustainable compliance will require more than "project tools."

Automate controls
There will be significant opportunities to leverage technology to automate controls and achieve improvements in control effectiveness. The automated control capabilities within existing applications are generally not fully utilized. In addition, there are important new areas where technology can enable controls. Segregation of duties and system security are two examples of near-term opportunities. While this may be considered to be in the category of "improvement," it is important to include the assessment of such opportunities in planning the technology investments and projects in year two and beyond.

Anticipate technology needs and issues
Certain events and activities can have a profound impact on internal control technology. Mergers and acquisitions, for example, will require integration of the two entities' IT systems — a daunting task even before one considers the internal control aspects. Fortunately, the SEC has acknowledged that it may be difficult to conduct an assessment of an acquired company's internal control over financial reporting in the period between the acquisition date and the date of management's assessment. In such cases, the acquired company may be excluded from management's report on internal control over financial reporting. However, this exclusion must be noted in the report as well as disclosed on Form 10-K or 10-KSB. Furthermore, companies may only omit an assessment of an acquired company's internal control over financial reporting for a period of no more than one year from the date of acquisition, and from no more than one annual management report on internal control over financial reporting.

Mergers and acquisitions will require integration of the two entities' IT systems — a daunting task even before one considers the internal control aspects.

No such grace period is granted when new technology is put into place, such as a large-scale enterprise resource planning (ERP) system. In fact, controls are going to need to be in place and functioning on day one. As such, the timing of technology rollouts will have to be carefully considered. If the system goes live during the fourth quarter, for example, management may be hard-pressed to assess and report on controls, and any control remediation and retesting will be virtually impossible.

As companies build their sustainable programs, continuous improvement will become more important. Improving financial monitoring and reporting will require technology enhancements, both to speed the process and improve quality. Since data is not knowledge, there will likely be an increased emphasis on analytics. Longer term, companies will likely be faced with challenges concerning standardizing and rationalizing their systems.

WHAT WILL YOU DO IN SARBANES-OXLEY YEAR TWO?

Among the positive outcomes of the first year of the Sarbanes-Oxley era — and there were many — is the valuable lessons learned by all those involved in the effort. The struggle to attain compliance helped create near unanimity among business executives that they don't want to — and can't afford to — endure this process again. So motivated, they will be inspired to fully integrate the principles of good governance and internal control into every corner of their organizations.

Year two provides a unique opportunity to leverage all that has been learned. As organizations move beyond compliance and toward sustainability, they will work to reduce unnecessary complexity and will strive to strengthen the link between internal control and financial reporting. These activities can potentially provide the multiple benefits of improved financial reporting, reduced risk, and decreased cost.

And while the concept of sustainability described in this paper refers only to long-term compliance with Sarbanes-Oxley sections 302 and 404, executives who act upon the guidance contained herein will also be laying the foundation for improvements in all areas of their business. Doing so, they will have taken what could have been a regulatory burden and turned it into a competitive advantage.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. Deloitte Touche Tohmatsu is an organization of member firms around the world devoted to excellence in providing professional services and advice, focused on client service through a global strategy executed locally in nearly 150 countries. With access to the deep intellectual capital of 120,000 people worldwide, Deloitte delivers services in four professional areas – audit, tax, consulting, and financial advisory services – and serves more than one-half of the world's largest companies, as well as large national enterprises, public institutions, locally important clients, and successful, fast-growing global growth companies. Services are not provided by the Deloitte Touche Tohmatsu Verein, and, for regulatory and other reasons, certain member firms do not provide services in all four professional areas.

As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other related names.

In the U.S., Deloitte & Touche USA LLP is the member firm of Deloitte Touche Tohmatsu, and services are provided by the subsidiaries of Deloitte & Touche USA LLP (Deloitte & Touche LLP, Deloitte Consulting LLP, Deloitte Tax LLP, and their subsidiaries) and not by Deloitte & Touche USA LLP. The subsidiaries of the U.S. member firm are among the nation's leading professional services firms, providing audit, tax, consulting, and financial advisory services through nearly 30,000 people in more than 80 cities. Known as employers of choice for innovative human resources programs, they are dedicated to helping their clients and their people excel. For more information, please visit the U.S. member firm's website at www.deloitte.com/us.

#4299