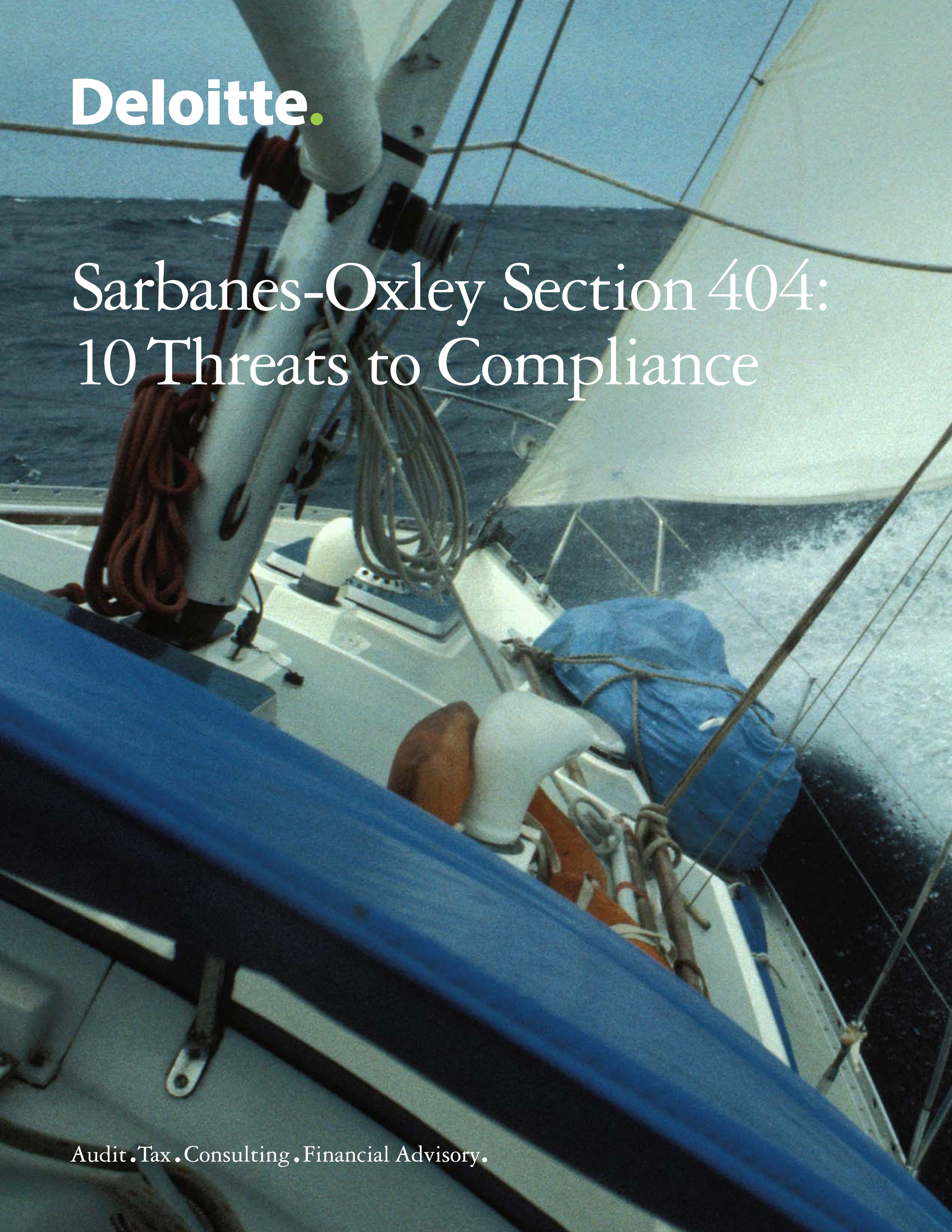
Deloitte.

Sarbanes-Oxley Section 404: 10 Threats to Compliance



Audit . Tax . Consulting . Financial Advisory.

Sarbanes-Oxley Section 404: 10 Threats to Compliance

For many organizations, successfully achieving compliance with section 404 of the Sarbanes-Oxley Act is proving to be much more challenging than first anticipated. Many companies underestimated the necessary scope of the documentation, evaluation, and testing efforts, as well as the staffing requirements, and they are now discovering unanticipated internal control issues.

Drawing on our experience assisting more than 800 organizations with their section 404 readiness efforts, we have identified 10 internal control issues that are often particularly challenging for management to address. For many organizations, these issues indicate a serious weakness in one or more of the key components of internal control defined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), the standard that most companies have adopted to assess the effectiveness of their internal control over financial reporting. If such flaws remain unresolved, they may prevent management from reporting that internal control over financial reporting is effective – and potentially warrant an adverse opinion from the company's independent auditors.

1. Lack of an enterprise-wide, executive-driven internal control management program

A strong, enterprise-wide, executive-driven internal control management program is essential to achieving section 404 compliance. Consider that a section 404 compliance project must encompass the company's overall control environment as well as every key process related to financial reporting throughout the organization, in all business units, divisions, and functions. Moreover, companies must annually repeat the section 404 assessment process, making it critical for this year's compliance project to lay the foundation for sustained compliance in the future. And because executive oversight of internal control is fundamental to COSO's concept of strong internal control, company leaders should take explicit responsibility for managing internal control over financial reporting in all areas of the organization.

The most crucial part of any internal control management program is its human resource component – the need to hire, develop, and effectively manage enough qualified control specialists to achieve sustained compliance. Finding the people to staff the initial compliance effort, while a major challenge in and of itself, is only the first step. Executives need to deploy a human resource strategy that will deliver a staffing model that will align the control specialists needed to deliver a sustained and efficient compliance process. This will require companies to consider how 404 control specialists will be organizationally aligned, define required competencies that are developed and maintained through training or recruiting programs, and develop and refine job descriptions and responsibilities. Through these actions, a company can establish a human resource infrastructure that will support the transition of its initial section 404 compliance efforts to a sustainable, culturally embedded process.

An effort of this magnitude cannot be sustained haphazardly or on a piecemeal basis. Rather, it must be driven from the top down through

10 Threats to Compliance

Companies working toward section 404 compliance should be especially alert to the following threats to compliance:

1. Lack of an enterprise-wide, executive-driven internal control management program
2. Lack of a formal enterprise risk management program
3. Inadequate controls associated with the recording of nonroutine, complex, and unusual transactions
4. Ineffectively controlled post-merger integration
5. Lack of effective controls over the IT environment
6. Ineffective financial reporting and disclosure preparation processes
7. Lack of formal controls over the financial closing process
8. Lack of current, consistent, complete, and documented accounting policies and procedures
9. Inability to evaluate and test controls over outsourced processes
10. Inadequate board and audit committee understanding of risk and control

As used in this document, the term "Deloitte" includes Deloitte & Touche LLP, Deloitte Consulting LLP and Deloitte Tax LLP.

a formal, executive-driven, enterprise-level program for internal control management that, among other things:

- is directed and monitored at the CFO/CAO level
- engages all relevant areas of the organization and covers all key processes that affect financial reporting, regardless of location
- establishes and applies a consistent internal control framework for assessing risks and formulating appropriate control objectives and activities
- promotes standards and approaches for documentation, control design evaluation, and control effectiveness testing
- continuously monitors the organization's state of compliance
- promotes sustained compliance through training and awareness
- incorporates communication protocols to keep executive management and the board of directors informed about internal control issues and remediation efforts
- considers the deployment of suitable technology to facilitate the achievement of the above attributes

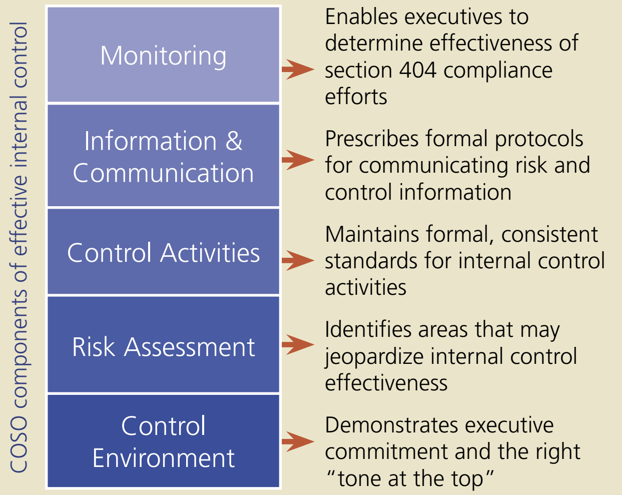
The lack of a strong enterprise-wide internal control management program threatens section 404 compliance in several ways:

- Absence of an enterprise-wide internal control management program casts serious doubt on executives' commitment to effective internal control. If an organization cannot show that such a program exists, its board of directors or independent auditors may suspect that the company's leaders lack the necessary focus and initiative to foster an effective control environment.
- Without an internal control management program to drive the enterprise-wide effort, a company may not only fail to detect a material weakness, which would result in an adverse opinion on the effectiveness of internal control over financial reporting from its independent auditors, but also jeopardize its ability to sustain compliance in future years.
- One of the key functions of an internal control management program is to inform executive management of the state of a company's internal control and the status of its section 404 compliance efforts. Executives who cannot demonstrate their knowledge of this information risk being unable to make the appropriate disclosures regarding changes to internal control over financial reporting required by section 302 of Sarbanes-Oxley.

Key questions to consider:

- *Is the organization's section 404 compliance project directed from the CFO/CAO level?* Section 404 practically requires that a company's most senior executives direct its compliance efforts and ongoing internal control monitoring program. The absence of involvement at this level could suggest inadequate top-level commitment to section 404 compliance.
- *Has executive management demonstrated full financial, logistical, and political support of the section 404 compliance effort?* Warning signs include the absence of a formal project management office, difficulty in obtaining dedicated resources for the compliance project, lack of executive inclusion in key section 404 compliance decisions, and an absence of management, divisional, and functional input into compliance efforts.

An effective internal control management program:


COSO components of effective internal control
Monitoring
Information & Communication
Control Activities
Risk Assessment
Control Environment

Enables executives to determine effectiveness of section 404 compliance efforts

Prescribes formal protocols for communicating risk and control information

Maintains formal, consistent standards for internal control activities

Identifies areas that may jeopardize internal control effectiveness

Demonstrates executive commitment and the right "tone at the top"

- *Does the company maintain formal, consistent, enterprise-wide standards for internal control management?* Consistency is the hallmark of a strong, enterprise-wide system of internal control. Companies that fail to set and communicate standards for internal control documentation, evaluation, testing, remediation, and monitoring throughout the organization can expect a hodgepodge of differently applied approaches and inconsistently derived conclusions in different business units, which will raise red flags during the independent auditor's internal control audit activities.
- *Is there a formal training program in place to teach employees to understand and fulfill their section 404 compliance responsibilities?* Companies cannot expect their employees to absorb correct behavior through osmosis, especially in an area as sensitive and judgmental as internal control over financial reporting.
- *Are there formal protocols for communicating internal control-related information among employees, management, and board members?* Explicit protocols should exist for communicating all relevant information about internal control to the appropriate people. Individual employees should be made aware of their responsibilities with regard to the compliance program and internal control; employees and corporate leadership must communicate around control deficiencies and remediation activities; and management should keep the board of directors informed as to the status of the company's compliance project.
- *Does the technology infrastructure adequately support section 404 compliance needs, both immediate and recurring, in all areas of the enterprise?* Control monitoring is central to the COSO internal control framework. Without proper technology to track and document internal control activities and related information, a company cannot claim to have satisfied COSO standards in its control monitoring responsibilities.

2. Lack of a formal enterprise risk management program

Critical to the success of any internal control management program is the establishment of an enterprise 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. A surprising number of companies lack such a process, relying on "seat of the pants" judgments instead of a disciplined and comprehensive analysis of risk resulting from informed reflection.

In our view, an effective risk management program should:

- determine the specific financial reporting risks that might arise as a consequence of the organization's business model, strategy, and operations. 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
- assess the potential impact of each identified risk on the integrity of financial reporting
- align each specific risk with one or more specific business processes or control environment areas in which that risk may occur
- assign responsibility for monitoring and controlling each risk, or set of risks, to the appropriate individuals
- include activities to monitor and report on changing risk conditions
- establish formal communication protocols regarding control performance and changes to the organization's risk profile

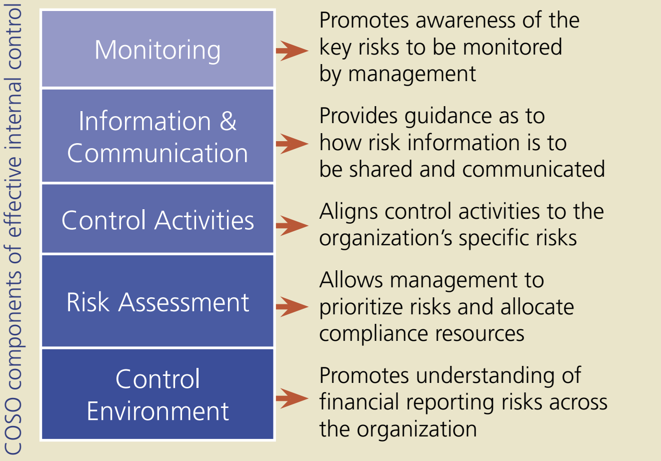
Implementing a formal risk assessment process helps sustain section 404 compliance in two ways. First, the existence of a formal process for identifying and assessing risks demonstrates that management is making every effort to apply the company's compliance efforts to the appropriate business areas. And second, a solid understanding of the organization's risk profile allows CxOs and board members to allocate their compliance resources more effectively, devoting the most attention to areas that represent the greatest risk. A formal risk assessment process also helps a company satisfy the NYSE requirement that the audit committee discuss its risk assessment and risk management policies with management.

We recommend that companies perform a risk assessment at least once a year to keep the organization's financial reporting risk profile in line with the evolution of the business. This assessment should occur early enough each year for the company to make appropriate changes before year-end. In addition, companies should re-evaluate its financial reporting risk profile every time it undergoes 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 assessment.

Key questions to consider:

- *Has the company assigned responsibility for performing the overall risk assessment to a specific group of people at the appropriate organizational level?* Just like the larger internal control program, the risk assessment program should belong to a particular group that is responsible for driving the process. Although the risk assessment group need not include members of executive management, it should wield enough influence to be able to guide the executive team's approach to internal control management.

An effective enterprise risk management program:


COSO components of effective internal control
Monitoring
Information & Communication
Control Activities
Risk Assessment
Control Environment

Promotes awareness of the key risks to be monitored by management

Provides guidance as to how risk information is to be shared and communicated

Aligns control activities to the organization's specific risks

Allows management to prioritize risks and allocate compliance resources

Promotes understanding of financial reporting risks across the organization

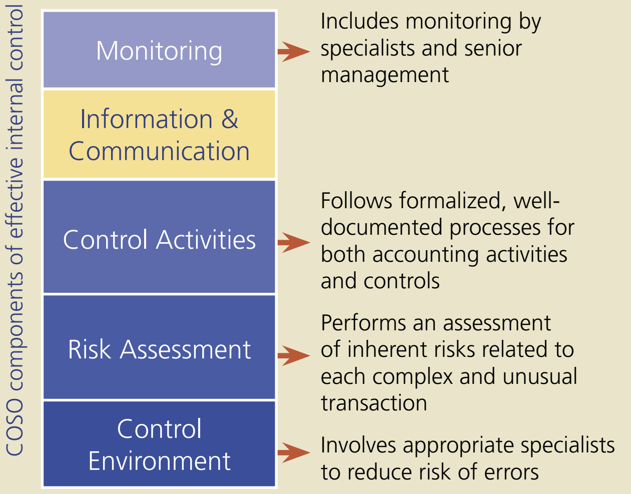
- *Are risks consistently prioritized, controlled, and communicated throughout the organization?* All areas of the business should share a common view of the company's key financial reporting risks, internal control objectives, and the associated control activities. A formal risk assessment process, supported by adequate communication and training, is the only way to uphold such enterprise-wide consistency.
- *Have specific risks been explicitly mapped to specific business processes and relevant control environment areas and, in turn, to the individuals responsible for performing these processes?* By mapping risks to specific processes, and those processes to particular people, a company can better define detailed controls over each process and appropriately assign responsibility for executing those controls. Conversely, an inability to precisely map risks to specific processes and individuals implies significant flaws in the company's risk management process.
- *Do employees understand the risks associated with their business areas and the processes they perform, and do they know how to execute the relevant control activities?* Effective risk management depends on effective communication to everyone who touches a process relevant to financial reporting or has a role in maintaining the overall control environment. Each person should thoroughly understand and consistently execute his or her internal control responsibilities, and each person should know how to bring internal control issues to his or her supervisor's attention. If rank-and-file employees are confused about their responsibilities, or if communication breaks down at any point along the chain of command, an organization cannot claim to maintain adequate internal control according to the COSO framework.
- *Does the supporting technology adequately collect, track, and maintain risk-related information?* Just as with the larger internal control program, the organization's risk management program must be supported by an adequate IT infrastructure.

3. Inadequate controls associated with the recording of non-routine, complex, and unusual transactions

Mergers and acquisitions, divestitures, valuations of assets, plant closures, pension accounting and complex compensation plans – these and other unusual, highly complex transactions present considerable financial reporting risks. However, many organizations lack the technical accounting knowledge to record complex transactions correctly, and even competent employees are unlikely to have much experience accounting for complex transactions that occur only occasionally in an environment of changing accounting requirements. Errors in recording such transactions can require a company to restate its reported results, which in itself is considered a control weakness and precludes a favorable section 404 report.

Exacerbating the problem is that many companies do not adequately document their process, if any, for the preparation or management review of complex transactions. Insufficient documentation of accounting procedures can sabotage attempts to properly reflect these difficult transactions and hinder efforts to apply corrections when needed. Also, inadequate internal control documentation can prevent management from assessing or demonstrating the effectiveness of controls over complex transactions. In either case, the organization exposes itself to the risk of an adverse opinion in its independent auditors' audit of internal control.

Effective reporting of complex and unusual transactions:


COSO components of effective internal control
Monitoring
Information & Communication
Control Activities
Risk Assessment
Control Environment

Includes monitoring by specialists and senior management

Follows formalized, well-documented processes for both accounting activities and controls

Performs an assessment of inherent risks related to each complex and unusual transaction

Involves appropriate specialists to reduce risk of errors

Key questions to consider:

- *Does the company involve appropriate subject matter experts to record complex transactions?* To get it right the first time, an organization that has conducted unusual, non-recurring, or other complex types of transactions should consider involving experienced specialists, whether in-house employees or outside consultants, when accounting for these transactions.
- *Has management appropriately assessed the competency of outside specialists engaged to assist the company?* An organization that hires outside specialists to account for complex transactions should document the capabilities of the specialists, the process by which they are engaged, and the protocols for monitoring their activities as part of the organization's overall control documentation procedures.
- *Does the company maintain, adequately document, and effectively disseminate standardized procedures to be followed for unusual and complex transactions?* Lack of adequate, timely documentation for such high-risk processes may be considered a control weakness in itself.
- *Does the organization maintain or subscribe to ongoing training programs to keep its accountants up to date on changes to SEC regulations, GAAP, and other transaction-reporting requirements?* Lack of an ongoing, company-wide training program around accounting standards and procedures can raise independent auditors' suspicions as to the competence of the company's accounting personnel.

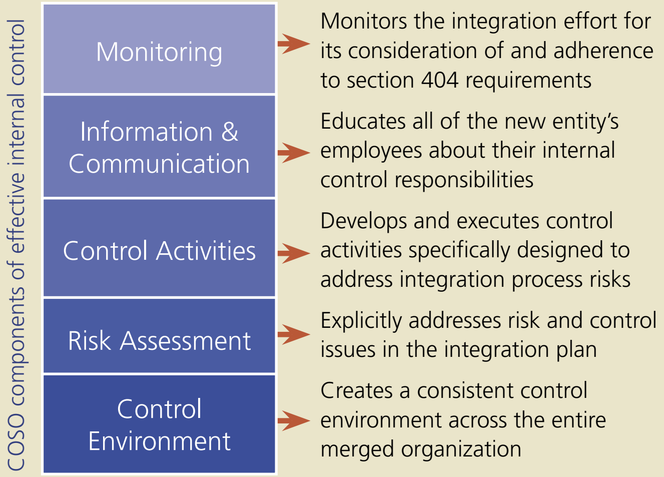
4. Ineffectively controlled post-merger integration

A merger or acquisition is one of the most significant of all business events. It's also one of the most difficult processes through which to maintain effective internal control. In the rush to get the combined entity up and running, companies often fail to properly address the myriad internal control issues that inevitably arise.

Blending two different sets of people, processes, and technologies into a seamless whole is notoriously difficult, especially when the new entity is under intense pressure to deliver market synergies as soon as possible. At the same time, every facet of the integration effort – employee training, system integration, data migration, process redesign – presents potential internal control risks, all of which occur in the same short period of time. An organization whose resources are already stretched thin by the market-level, back-office, and management aspects of the integration frequently relegates internal control considerations to the back burner. Unfortunately, this opens the door to significant control weaknesses and gaps that may not be discovered until late in the section 404 compliance process.

Merging companies often also neglect to explicitly address the need to establish a consistent internal control environment across the entire consolidated entity. Again, the drive to complete the high-impact cost reduction aspects of the integration can eclipse internal control issues and the need to fully understand and integrate the acquired company's accounting policies and procedures. The probable result: Widely varying controls in different sections of the enterprise, each representing a previously merged or acquired entity, that point to management's failure to properly establish an effective system of internal control throughout the organization.

An effectively controlled integration:


COSO components of effective internal control
Monitoring
Information & Communication
Control Activities
Risk Assessment
Control Environment

Monitoring	Monitors the integration effort for its consideration of and adherence to section 404 requirements
Information & Communication	Educates all of the new entity's employees about their internal control responsibilities
Control Activities	Develops and executes control activities specifically designed to address integration process risks
Risk Assessment	Explicitly addresses risk and control issues in the integration plan
Control Environment	Creates a consistent control environment across the entire merged organization

Key questions to consider:

- *Does the organization have a history of significant M&A activity?* Even a single large merger or acquisition generates risks that may lurk unnoticed until an internal control audit, with the number of accumulated risks increasing with each additional transaction.
- *Is the company undergoing a merger or acquisition at the same time as its section 404 compliance project?* It's hard to imagine two bigger, more complex projects than a post-merger integration and a section 404 readiness effort. Doing both at once demands an exceptionally intense focus on internal control issues, both in performing the integration activities and in establishing a uniform control environment thereafter. Critical to success is to perform a risk assessment of the effect of integration activities on section 404 compliance, and then to build specific plans for addressing section 404 issues into the overall integration strategy.
- *Are executives fully aware of M&A activities undertaken by individual business units?* If not directed at the corporate level, an independently conducted M&A and integration may compromise a business unit's adherence to enterprise internal control standards.
- *Has the company acquired entities with very different IT systems from its own?* No two companies have identical technology infrastructures, and the bigger the difference, the greater the risk of the integration process.
- *Has the company established clear processes for producing the first externally reported numbers following the merger or acquisition?* Accurate reporting under what is often a very compressed integration timeframe depends on establishing and enforcing clear expectations around the consolidation process and the related controls.

5. Lack of effective controls over the IT environment

Enabling technologies for executing and reporting transactions are ubiquitous in modern organizations, and technology plays a critical role in the control environment. But even as companies have become more dependent on technology to execute and document transactions, the technology itself has become more complex and more difficult to maintain. What's more, section 404 marks the first time that companies have been legally required to evaluate and test their controls in the IT environment in such depth and detail. Many organizations, systematically examining their IT control environment for perhaps the first time, are uncovering pervasive control issues that may compromise section 404 compliance. The more complex a company's IT environment, and the less attention it has previously paid to IT controls, the more IT control gaps are likely to exist – and the more challenging and time-consuming they will be to fix.

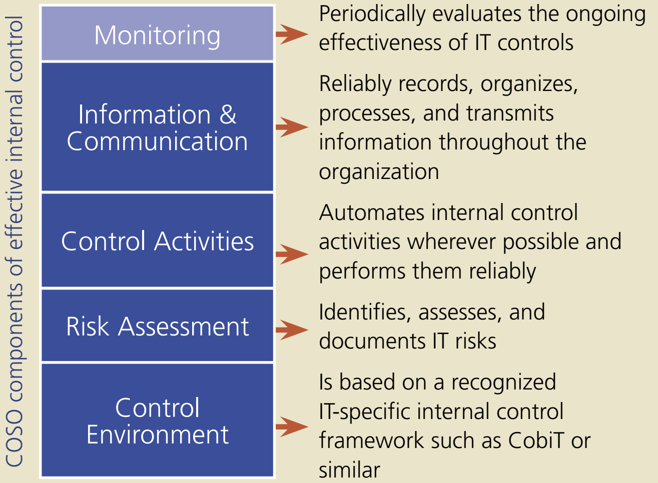
Considering the ubiquity of technology in transaction processing, flaws in IT controls design, execution, and governance can sabotage reliable financial reporting in countless ways. Common areas of pervasive weakness include:

- systems development, implementation, maintenance, and change management
- data conversion and system interface controls
- security technologies, protocols, and administration
- third-party IT service providers

Key questions to consider:

- *Has the organization established an IT-specific internal control framework to guide its section 404 compliance activities with respect to IT?* An IT-specific internal control framework provides vital structure to an organization's effort to develop and maintain effective internal control in its IT environment. Failure to identify such a framework may indicate that the organization has failed

A well-controlled IT environment:


COSO components of effective internal control
Monitoring
Information & Communication
Control Activities
Risk Assessment
Control Environment

Monitoring	Periodically evaluates the ongoing effectiveness of IT controls
Information & Communication	Reliably records, organizes, processes, and transmits information throughout the organization
Control Activities	Automates internal control activities wherever possible and performs them reliably
Risk Assessment	Identifies, assesses, and documents IT risks
Control Environment	Is based on a recognized IT-specific internal control framework such as CobiT or similar

As used in this document, the term "Deloitte" includes Deloitte & Touche LLP, Deloitte Consulting LLP and Deloitte Tax LLP.

to examine IT controls as systematically or as deeply as required to support section 404 compliance. One possible IT-specific control framework to build upon is the CobiT framework, described by the IT Governance Institute in its 2000 publication, "Control Objectives for Information and Related Technology." While the full CobiT framework goes far beyond section 404 compliance requirements, companies seeking guidance regarding IT controls would be well advised to customize the applicable portions of CobiT for their own particular section 404 compliance needs.

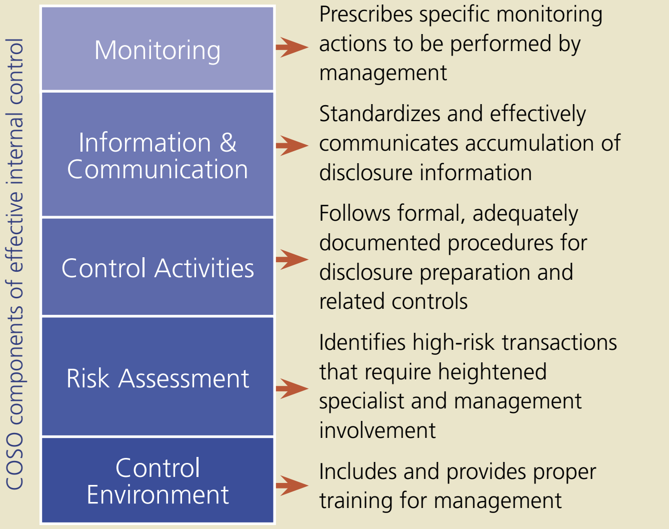
- *Is the IT environment highly customized?* Custom-built applications and platforms are a fertile ground for internal control issues for two reasons. One, the original technology's vendor may not be able or willing to provide technical support once its product has been significantly modified. And two, no matter how competent a company's IT personnel or service providers, there's always a much higher risk of errors in new, untried software than in standardized, widely used, and well-tested software.
- *Does the IT department have a high turnover rate?* Technology specialists, as a group, tend to gravitate toward best-of-breed, sophisticated, cutting-edge IT environments. A high turnover rate among IT professionals may indicate their dissatisfaction with dated, refractory technology whose unreliability could compromise internal control effectiveness.
- *Is there a large backlog of outstanding program maintenance requests?* If your IT professionals, though competent, are having trouble keeping up with program maintenance requests, chances are that the systems are overly complex and tedious to work with, casting doubt on their reliability with regard to internal control.
- *Has the company needed to extensively rework or retrofit an installed ERP system(s)?* Badly designed or incompletely activated ERP controls can create significant internal control gaps.
- *Does the company rely on disparate legacy systems to manage financial reporting?* Every time information needs to be altered for purposes of inter-system compatibility, the risk of introducing errors goes up. In addition, high variability in a company's financial applications increases both the time required to consolidate the information at year-end and the effort of managing risks and controls for each individual application.
- *Have formalized, consistent IT standards been established across all areas of the organization?* The absence of clear IT standards prescribing enterprise-wide policies for applications, infrastructure, operating protocols, and other IT-related factors encourages variability among different areas of the business, thereby increasing complexity and risk.
- *Are significant manual control activities required to manage the results provided by information systems?* Employees who feel they cannot rely on a company's technology may use manual processes to compensate for IT weaknesses. Not only are such manual processes labor-intensive and inefficient, but they are inherently riskier than automated processes due to irreducible human error.
- *Do the organization's IT processes maintain an adequate segregation of duties?* Technology can make it easy for one person to perform the work of many – but it also raises the risk of concentrating too much responsibility in one person's hands. Effective segregation of duties is therefore crucial to maintaining strong internal control over technology-enabled processes. To satisfy section 404 requirements, organizations must be able to document the existence and enforcement of appropriate segregation of duties with regard to IT. This may need to take place as part of an overall effort to improve information security controls, which is often more tedious and time-consuming than most companies expect.

6. Ineffective financial reporting and disclosure preparation processes

The accelerating rate of regulatory and legal change in the past few years has increased the number and complexity of required financial disclosures, a trend that shows no sign of slowing. However, some companies may not possess the in-house technical accounting skills needed to prepare financial disclosures accurately. The problem is often compounded by the lack of a solid, rigorous process for collecting and organizing the information required to prepare the disclosures in the first place. Even companies that do follow an established disclosure preparation process may not adequately document it or properly assess and test the design of the related controls. Many, in fact, have historically relied on their independent auditors in this area.

Now, Sarbanes-Oxley section 404 has made the financial disclosure preparation process, as well as the completeness and accuracy of the disclosures themselves, subject to the independent auditor's internal control audit procedures. Realizing this, many organizations are scrambling to develop or buy the specialized accounting capabilities required to produce disclosures that will stand up to a section

An effective financial disclosure preparation process:



Monitoring	Prescribes specific monitoring actions to be performed by management
Information & Communication	Standardizes and effectively communicates accumulation of disclosure information
Control Activities	Follows formal, adequately documented procedures for disclosure preparation and related controls
Risk Assessment	Identifies high-risk transactions that require heightened specialist and management involvement
Control Environment	Includes and provides proper training for management

404 attestation. Absent these capabilities, as well as adequate documentation of the disclosure preparation process and the associated controls, a company incurs a serious risk of falling short of section 404 compliance in this area.

Key questions to consider:

- *Has management needed assistance to prepare disclosures in previous years?* Past reliance on outside specialists is a good sign that an organization lacks the in-house capabilities to adequately prepare financial statement disclosures.
- *Have the independent auditors recommended changes to the footnotes during the audit process?* Section 404 requirements make it inadvisable for a company to rely on its independent auditors to assist with the development of financial disclosures or to identify financial disclosure weaknesses.
- *Have adjustments to disclosures often been proposed in previous years?* A history of frequent adjustments to financial disclosures may indicate that a company lacks the proper skills and/or controls to prepare them correctly the first time.
- *Does the company have formal documentation of its disclosure process and controls?* As a significant business process in itself, the disclosure development and review process should be documented to enable management to explicitly evaluate the design and test the operating effectiveness of the controls related to this process.

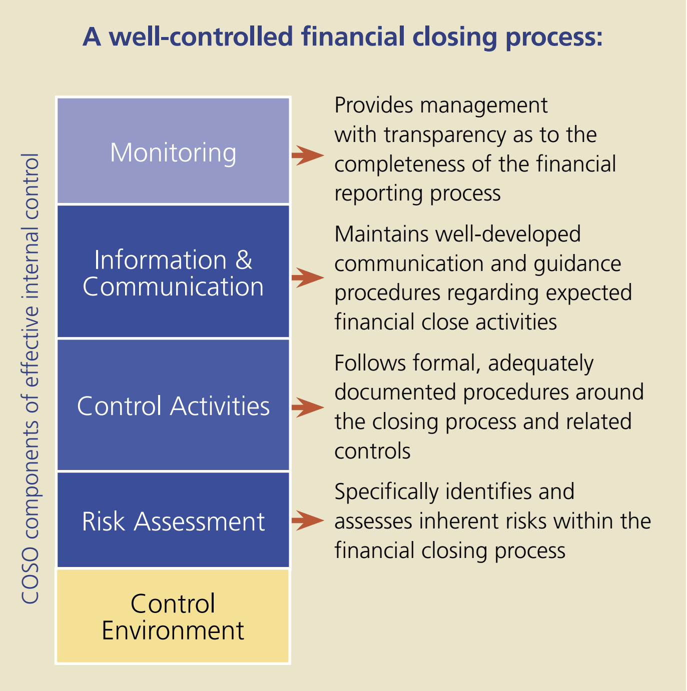
7. Lack of formal controls over the financial closing process

The financial closing process, as the final step to producing an official financial report, is an inherently high-risk activity, made even more so by its extreme complexity. The organization must obtain, analyze, and consolidate information from multiple sources, carry out reconciliations, make any necessary adjustments, and perform many other complicated, often highly judgmental tasks, all in a very short time. Under these circumstances, the process can easily degenerate into a fire drill in which following rigorous internal control procedures is the last thing on anyone's mind.

To avoid the damage a poorly controlled financial close process can inflict on section 404 compliance, companies should establish formal procedures for executing and documenting both the financial closing activities themselves and their associated control activities. These procedures must be followed under all circumstances, even – indeed, especially – when time pressures or accounting intricacies tempt people to slack. The goal is to be able to document the closing process in enough detail to enable management to effectively evaluate the design of closing process controls and test their operating effectiveness. In addition, adequate documentation of the closing process and the related controls enables the independent auditors to perform their required walk-throughs for the section 404 attestation.

Key questions to consider:

- *Are closing activities performed in a timely manner?* Perhaps the most obvious sign of an ineffective closing process is a chaotic, eleventh-hour rush to get the job done on time. Not only does this increase the risk of control lapses, but it also suggests a general negligence around organization and planning that may reflect badly on the company's overall control environment.
- *Does the organization formally prescribe and document all activities in the financial closing process, from initial information-gathering to the final report production and management review process?* A company that cannot produce documented evidence for a formal financial closing process has little chance of convincing its independent auditors that an effective process in fact exists.
- *Does the organization formally prescribe and document all control activities related to the financial closing process?* Here, too, lack of documentation will cripple a company's ability to demonstrate effective controls over the closing process.



A well-controlled financial closing process:

COSO components of effective internal control

Monitoring → Provides management with transparency as to the completeness of the financial reporting process

Information & Communication → Maintains well-developed communication and guidance procedures regarding expected financial close activities

Control Activities → Follows formal, adequately documented procedures around the closing process and related controls

Risk Assessment → Specifically identifies and assesses inherent risks within the financial closing process

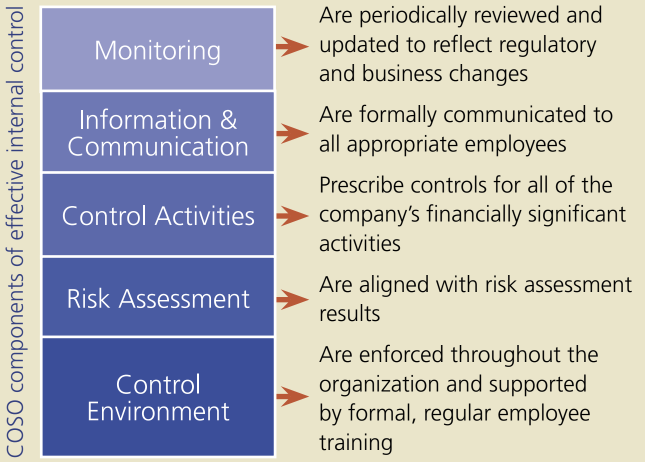
Control Environment

8. Lack of current, consistent, complete, and documented accounting policies and procedures

The more current, consistent, and complete a company's accounting policies and procedures, the easier they are to evaluate and document, and the more effectively the company can control associated risks. At some organizations, however, accounting policies and procedures may not be consistently and systematically reviewed and revised during times when changes to the business and to generally accepted accounting procedures (GAAP) render them obsolete. Policies and procedures may also be inconsistently designed and/or applied in different parts of the enterprise, fail to cover the full set of processes relevant to financial reporting, or lack the necessary range of guidance and direction. Any of these weaknesses can be fatal to a company's section 404 compliance efforts.

Companies with global operations are especially vulnerable to risks arising from weaknesses in accounting policies and procedures. Much of a global company's accounting is necessarily performed by non-U.S. personnel, many of whom may have only limited skill and experience in applying U.S. GAAP. Strong guidance through a standard set of accounting policies and procedures is an important defense against errors arising from uncertainty or inexperience.

Effective accounting policies and procedures:



COSO components of effective internal control	
Monitoring	Are periodically reviewed and updated to reflect regulatory and business changes
Information & Communication	Are formally communicated to all appropriate employees
Control Activities	Prescribe controls for all of the company's financially significant activities
Risk Assessment	Are aligned with risk assessment results
Control Environment	Are enforced throughout the organization and supported by formal, regular employee training

Key questions to consider:

- *Does the company have a standard manual of accounting policies and procedures, and is there a process for updating it regularly?* The absence of a standard manual and a process for keeping it current are sure signs of ineffective oversight over accounting policies and procedures.
- *Are transactions recorded in a timely manner?* Unclear, incomplete, or otherwise inadequate policies and procedures may lead to sluggish transaction processing, as employees spend time cross-checking their activities with each other and with supervisors.
- *Has the organization needed to make frequent and/or highly significant prior-period adjustments?* Large accounting errors, or a pattern or recurring errors, can indicate flaws in the accounting policies and procedures governing those areas.
- *Does the organization provide regular training and communications regarding changes to accounting policies and procedures?* The absence of regular, formal training in new or revised accounting policies and procedures increases the risk that policies or procedures will not be applied in a manner consistent with management's expectations. In addition, the lack of timely and regular training around accounting policies and procedures may suggest a lack of management commitment to establishing an effective control environment.

9. Inability to evaluate and test controls over outsourced processes

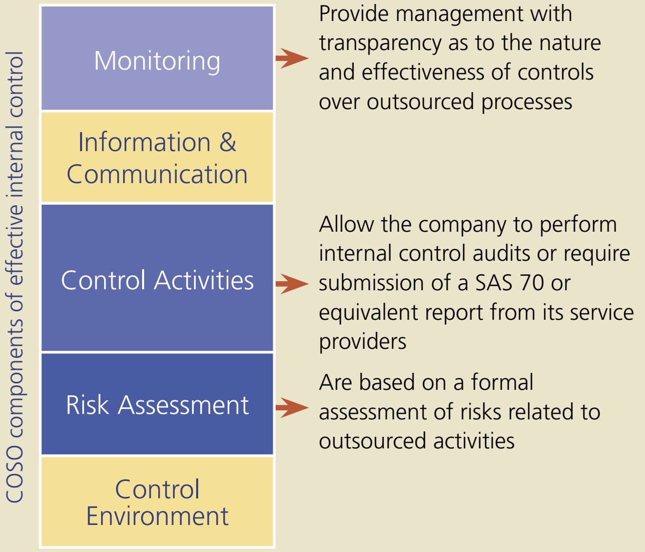
Many companies in recent years have aggressively outsourced fundamental business processes that have a large potential impact on financial reporting, such as sales order entry, payroll, inventory, accounts payable, and the like. Having outsourced these activities, however, companies often tacitly delegate the responsibility for internal control to the outsourcer as well. Executives seldom include clear expectations around internal control performance in service contracts, and also often fail to establish the contractual right to perform internal control audits or request a SAS 70 or equivalent report. The resulting lack of transparency into outsourcers' internal control environments has seriously hampered many organizations' section 404 compliance efforts, as they struggle to identify, document, and evaluate the internal control processes that occur – or not – at outside service providers.

If a company cannot obtain adequate information to evaluate controls over certain outsourced processes, management cannot report on the effectiveness of those controls. This may result in a qualified opinion due to a scope limitation on the independent auditors' section 404 report, depending on the significance of the outsourced activities for which no assertion can be made. While not as damaging as an adverse opinion due to a material weakness, a scope limitation can still prompt prejudicial speculation as to why a company failed to examine its system of internal control in its entirety.

Key questions to consider:

- *Does the company maintain a complete inventory of its outsourced relationships?* Effective internal control over outsourced activities begins with knowing exactly what processes are outsourced and

Effective controls over outsourced processes:



COSO components of effective internal control	
Monitoring	Provide management with transparency as to the nature and effectiveness of controls over outsourced processes
Information & Communication	
Control Activities	Allow the company to perform internal control audits or require submission of a SAS 70 or equivalent report from its service providers
Risk Assessment	Are based on a formal assessment of risks related to outsourced activities
Control Environment	

where. Without an up-to-date, complete inventory of service contracts and providers, an organization cannot even confidently identify, let alone control, risks that may arise within outsourced processes.

- *Do business units enter into outsourced activities independently of central management?* Frequent ad hoc formation of service contracts in different parts of the organization strongly suggests the lack of a common framework of corporate standards for managing and reporting on outsourced relationships. In turn, the absence of enterprise-level oversight of outsourced relationships may imply that management lacks the commitment or ability to fulfill their internal control responsibilities regarding their outsourced activities.
- *Do service contracts include the right to perform an internal control audit or request a SAS 70 or equivalent report?* Companies that neglect to obtain such contractual rights may experience varying degrees of difficulty in obtaining the information needed to evaluate and assert on internal control over outsourced activities. Overseas service providers tend to be especially recalcitrant in this regard.
- *Does the company have a process to monitor the level of service that it receives, including a procedure to monitor changes to the outsourced providers' environment?* Companies should have a predetermined process to monitor vendors' compliance with service level agreements. The monitoring procedures should include reviews of the vendor's internal control processes and the associated costs (if deemed material). Without procedures to monitor service providers' quality and effectiveness, the company may be unable to detect any deterioration in service or controls over time.

10. Inadequate board and audit committee understanding of risk and control

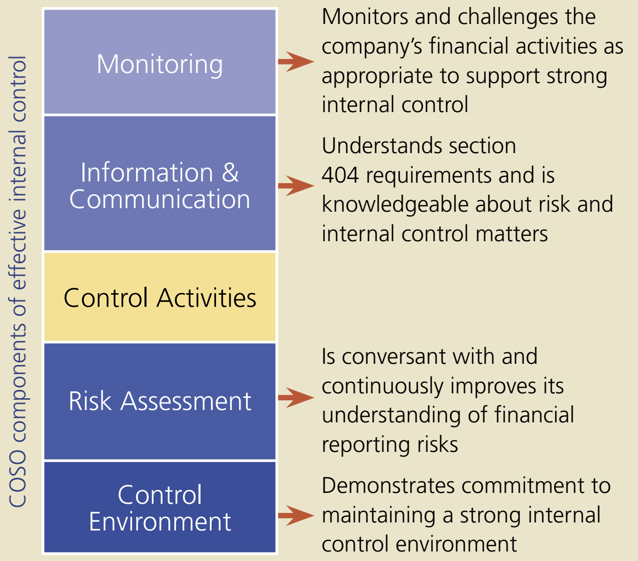
Sarbanes-Oxley has greatly increased the degree to which boards of directors, and especially audit committees, are expected to understand the nature of financial reporting risks and the function of internal control. The SEC considers board-level understanding of risk and control to be so important that it requires a company to either disclose that it has a designated "financial expert" on the audit committee or explain why it does not. In addition, the independent auditors must evaluate the effectiveness of the audit committee's oversight of the company's external financial reporting and internal control over financial reporting.

If the audit committee cannot establish that its members understand risk and control, the financial reporting process, and their responsibilities around section 404 compliance and other provisions of the Sarbanes-Oxley Act, the independent auditors are unlikely to have much confidence in the effectiveness of the audit committee's oversight of internal control. Board members should therefore be well versed in the general requirements for section 404 compliance, and they should be familiar with their own, management's, and the independent auditors' key responsibilities in the attestation process. They should also be prepared to examine management's internal control testing process for rigor and comprehensiveness, paying particular attention to areas in which management's conclusions differ from those of the independent auditors. Most importantly, all board and audit committee members should show an ongoing commitment to increasing their understanding of risk and control, and continuously strive to uncover and resolve issues that could compromise the organization's internal control environment.

Key questions to consider:

- *Do board and audit committee members review and appropriately challenge management's performance of section 404 compliance procedures?* Even if management has admirably discharged its section 404 compliance responsibilities, an audit committee that leaves compliance entirely in management's hands risks receiving a negative evaluation on the auditors' section 404 attestation report for its lack of meaningful oversight.
- *Does the company maintain formal, ongoing education programs for boards and audit committees to establish and maintain basic risk and control competencies?* Board and audit committee members do not necessarily need to bring a great deal of risk and control experience to the job. However, they do need to become reasonably conversant with risk and control issues and periodically refresh their knowledge to reflect regulatory and environmental changes. Implementing a formal board and audit committee training program is a good way to accomplish this as well as demonstrate top-level commitment to high standards of internal control oversight.

An effective board and audit committee:


COSO components of effective internal control
Monitoring
Information & Communication
Control Activities
Risk Assessment
Control Environment

Monitors and challenges the company's financial activities as appropriate to support strong internal control

Understands section 404 requirements and is knowledgeable about risk and internal control matters

Is conversant with and continuously improves its understanding of financial reporting risks

Demonstrates commitment to maintaining a strong internal control environment

Contacts

New York, NY
Henry Ristuccia, 212-436-4244

Parsippany, NJ
Karl Hersch, 973-683-6883

Boston, MA
E. J. Landry, 617-437-2157
Bob Updaw, 617-437-3570

McLean, VA
Monte Zaben, 703-251-1819

Atlanta, GA
Terry Cowles, 404-631-2999
Jeffrey Lund, 404-220-1083

Glen Mills, PA
Lee Dittmar, 610-479-3952
Todd Oken, 610-479-3638

Detroit, MI
Todd McGowan, 313-396-3407

Cleveland, OH
David Stahler, 216-589-1406

Cincinnati, OH
David Brainer, 513-784-7230
Tom Haberman, 513-784-7170

Chicago, IL
John Gimpert, 312-946-2591
Scott Rosenfelder, 312-946-2704

Houston, TX
Robert Penshorn, 713-982-2697

Irving, TX
Frank Borgsmiller, 469-417-3625

San Francisco, CA
Edwin Byers, 415-783-4402

Costa Mesa, CA
Sean Peasley, 714-436-7410

San Ramon, CA
Richard Woodward, 650-372-4595

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.

Member of
Deloitte Touche Tohmatsu