

The CIO's perspective

Introduction

In a survey of executives from 19 Fortune 100 companies that was conducted by *CIO* magazine, most viewed compliance with Sarbanes-Oxley as a finance issue, not a systems issue.¹ The *CIO* article went on to state that those executives “are dangerously mistaken ... Since information technology systems are used to generate, change, house and transport that data, chief information officers have to build the controls that ensure the information stands up to audit scrutiny.”²

This issue of *InSights* has been developed to help audit committee chairs gain a deeper understanding of:

- The interaction between the chief information officer (CIO) and the audit committee, the board of directors, internal and external auditors, and other corporate functions
- The impact of Sarbanes-Oxley compliance on the information technology (IT) function
- The IT general-control areas that represent the greatest areas of risk for the company
- The questions that audit committees should be asking their CIOs

In order to better understand the nature of the IT function, Tapestry Networks spoke with the CIOs of 12 companies that are among those represented by members of the Audit Committee Leadership Network in North America, the European Audit Committee Leadership Network, and the North Central and Mid-Atlantic Audit Committee Networks:

- Jean-Michel Ares, Vice President and Chief Information Officer, The Coca-Cola Company
- John Avampato, Vice President and Chief Information Officer, Newell Rubbermaid
- Brian Bonner, Vice President and Chief Information Officer, Texas Instruments
- Joseph Cleveland, Chief Information Officer, Lockheed Martin
- Robert DeRodes, Executive Vice President and Chief Information Officer, The Home Depot
- Brian LeClaire, Vice President and Chief Technology Officer, Humana
- John Leggate, Group Vice President and Chief Information Officer, British Petroleum
- Beth Perlman, Senior Vice President and Chief Information Officer, Constellation Energy
- Gary Reiner, Senior Vice President and Chief Information Officer, General Electric Company
- Glen Salow, Executive Vice President and Chief Information Officer, American Express
- Brad Tobin, Vice President and Chief Information Officer, FirstEnergy Corporation
- Carl Wilson, Executive Vice President and Chief Information Officer, Marriott International

¹ Ben Worthen, “Your Risks and Responsibilities,” *CIO*, May 15, 2003, <http://www.cio.com/archive/051503/rules.html>

² Ibid.

Executive summary

- **Section 404: An unexpected source of value** (pages 2-5)

CIOs found value in Section 404 compliance. As one CIO noted, *“this was lots of work, but we had good outcomes.”* Section 404 brought discipline to the implementation and documentation of essential controls, a more uniform application of policies, and an identification of gaps in processes.

- **Losing sleep: CIOs most concerned about access controls** (pages 5-6)

The Public Company Accounting Oversight Board’s Auditing Standard Number 2 outlined four categories of general IT controls – access to programs, computer operations, program changes, and program development. CIOs overwhelmingly agreed that access to programs was the area of greatest risk for their companies, with program changes following in second place.

- **Relationships evolving, but not with the audit committee** (pages 6-8)

Sarbanes-Oxley has brought very little change to the relationship between CIOs and audit committee members. Some audit chairs do not meet with the CIO; that lack of direct communication may create a risk for audit chairs. Boards are becoming more IT savvy, but may lack deep technical expertise. One CIO noted the benefits of engaging more CIOs in corporate governance and asked if boards might require certified technology experts similar to Sarbanes-Oxley’s mandate for financial experts.

- **Big questions: What should the audit committee be asking the CIO?** (page 8-9)

CIOs shared questions they think audit committees should be asking to gather needed information. For example, how does IT contribute to shareholder value? CIOs should be able to benchmark their company’s performance against industry best practice.

Section 404: An unexpected source of value

CIOs were generally positive when asked about the value of Section 404. While some felt that coming into compliance took up too much time (one CIO remarked, *“When I close my eyes at night, I see Section 404”*) most CIOs thought that compliance with Section 404 was a positive move for their companies. As one CIO noted, *“Section 404 is insisting on things that we should be doing for the business anyway; we have not done one thing for Sarbanes-Oxley that doesn’t make good business sense.”*

Section 404 as catalyst for best practices

CIOs were in agreement that Section 404 brought a needed level of discipline and forced a deadline to complete work that makes good business sense. One said, *“We needed to be doing control work anyway and this gives us a framework for it.”* Another noted, *“It makes you do things that are good practice but never hit your ‘to-do’ list.”* CIOs mostly agreed that the actions taken to comply were positive, even if the work was not entirely different from that which the company was already completing. One CIO noted, *“This work was well underway before Sarbanes-Oxley, but [the legislation] added rigor to the process and encouraged us to take a deeper look into the controls.”*

The actions taken for Section 404 were beneficial for IT departments in that CIOs took a “big picture” look at the systems in use across business units and functional lines. In the past, systems often grew faster than IT departments could document them. The requirements of Section 404 have forced a complete understanding and documentation of the systems in place. While CIOs reported that this process has been time consuming and tedious, it has resulted in more streamlined and secure systems that will benefit business beyond required compliance. As one CIO explained, “Section 404 is making us do some things that we have been doing and other things that we needed to be doing. Policies that were differentially adhered to in implementation [across the business units] are now being standardized.”

While the CIOs agreed that coming into compliance with Section 404 was generally a positive exercise, they were not sure if it was possible to quantify the benefits to the company. One CIO said, “This was good for business in general. This was a lot of work and does not drive earnings per share in the short term, but it will in the long term, I hope.” Another CIO said, “This is not a case of seeking a tangible return, but it is what we should have been doing all along.”

Variations in compliance experiences

The experience of compliance with Section 404 was not uniform for all CIOs. At some companies, compliance appears to have been straightforward. At others, compliance was more disruptive to existing initiatives. Three factors affected the Section 404 compliance effort:

- **Regulation:** The compliance workload was less in companies that had a high level of regulation before the enactment of Sarbanes-Oxley. As one CIO said, “This was just another layer of regulation ... given the vast array of supervisory bodies that oversee us, we already had these controls in place.”
- **IT centralization:** Centralized IT systems were easier for CIOs to document and test. As one CIO noted, “compliance was easy, and we had very minor issues since we are on a single system. Having only one process and one system makes the compliance process easier.”
- **Outsourced operations:** While operations may reside outside of the company, the control risks and compliance responsibilities of outsourced entities are still within the company. CIOs of companies which utilize outsourced operations had to take more steps to complete Section 404 compliance.

Since IT is increasingly important in driving business results, audit chairs may worry about the opportunity cost of Section 404 compliance, especially in companies whose CIOs were required to spend a greater-than-average amount of time on compliance. Further, given that it is easier to document controls in centralized IT environments, audit chairs may also question whether Section 404 will encourage companies to centralize the IT function. The extra expense involved in documenting outsourced IT operations may lead to a push to bring IT back in-house, but audit chairs may want additional evidence that such a move is good for the company in addition to easing the compliance burden on the IT department.



Table 1. Complexity variation in Section 404 compliance.

| Factor | Less Complex | More Complex |
|------------------------------|---|---|
| Regulation | High: CIOs in highly regulated industries reported that Section 404 brought no real change in the level of required documentation and testing. | Low: Section 404 compliance required more work by CIOs in less-regulated industries since much of the system documentation was new. |
| IT centralization | Centralized: CIOs perceived there to be less risk inherent in more streamlined systems, which had fewer systems to be documented. | Decentralized: More effort was required for companies whose IT systems were dispersed. One CIO said, <i>“You cannot control whether a message is fully understood by all users in remote locations.”</i> |
| Outsourced operations | Less outsourcing: The amount of work required of the CIO decreased as the amount of outsourcing decreased. | More outsourcing: Companies needed to order SAS 70 reports, which rate service organizations’ processing of transactions. This step increased the workload and cost. |

Budget not an issue: But was there a hidden cost?

CIOs indicated that budget was not a barrier; all received what they needed this year to complete Section 404 reporting. One CIO stated, *“The cost/benefit calculation of Sarbanes-Oxley is justifiable, because we will not be in business if we are not in Section 404 compliance.”* Another CIO noted that, *“the budget is always an issue, but it cannot be an issue when it comes to [Section 404], so we found a way around it. We always want to do more than what we have the resources to support.”*

While CIOs were relieved to have the budgets needed for compliance, only time will tell whether these required projects were completed at the expense of future IT projects. Audit chairs might ask their CIOs as to which projects, if any, were put on hold this year due to the time and expense invested in compliance.

Section 404 year two: Seeking sustainability

A few CIOs compared Section 404 compliance efforts with the Y2K project in the amount of preparation needed and the scope of effort involved. One CIO described how both efforts required *“senior-level attention to the issue, tedious details of what the efforts would entail, and good program management to pull it off.”* However, *“the cost structure [of the two efforts] differs in that Section 404 is ongoing.”* The continuous nature of Section 404 highlights the interests of the CIOs to learn how to make Section 404 compliance a sustainable process rather than a short-term project.

CIOs agreed that because controls have now been identified, year two should be less time consuming. Many CIOs pointed out that identifying key controls had taken more time than testing those controls. One CIO observed that knowing what was important, how to measure it, and how to document it represented *“a 25-30% time savings for year two.”* This CIO noted that *“maybe 50-60% of the work goes away in year three, but some portion always stays.”*

CIOs are also interested in automating their Section 404 efforts. Many hope to put into place sustainable practices that will require far less manual work than was required during year one. For example, one company converted all business units to the same financial platform to streamline consolidation of financial statements, while another CIO created “*methodologies, tool kits, and flowcharts*” to make the process more automated in year two. CIOs were glad to have the first year of Section 404 behind them, with one noting, “*Once you know the controls are in the system and they are the right ones, you sleep better at night.*”

Losing sleep: CIOs most concerned about access controls

In March 2004, the Public Company Accounting Oversight Board issued the first standard for conducting audits of internal controls in an audit of financial statements. This standard, Auditing Standard Number 2, gives a framework with four categories of IT general controls:

- **Access to programs:** Controls governing access rights granted to employees for systems and programs
- **Computer operations:** Controls designed for the general computing environment, such as for data management, business continuity, and disaster recovery
- **Program changes:** Controls developed for amendments to existing systems and programs
- **Program development:** Controls pertaining to the implementation of new systems and programs

The IT general controls are intended to act as a framework over all aspects of computerized processing and must be in place for reliance on automated operations. Taken together, the general controls define the IT systems that are involved in the financial reporting process.

Overwhelming focus on access controls

Despite the fact that a lot of attention is justifiably paid to IT topics such as viruses, firewalls, and systems recovery, only one of the twelve CIOs Tapestry Networks spoke with identified external threats as the number one IT risk area for the company. Ten thought access controls represent the area of greatest risk. Access controls ensure that only authorized individuals can execute financial transactions and that electronic and physical access to information and assets is restricted. When a company hires, fires, or promotes an employee, the access that individual has to IT systems must be updated.

In discussing the importance of access controls, one CIO brought up the risk inherent in the fact that large amounts of data can be taken quickly, and without leaving a trail. He said, “*I worry not just that someone will gain access to systems ... it is the ease in transferring large amounts of data onto very small devices. This can happen so quickly today that we need to catch acts [of theft] fast.*”

Program change controls were also identified as a substantial risk area by a number of CIOs, with one noting, “*Whenever you change a steady-state environment, you introduce risks.*” Change controls are those that assure system changes are approved by the correct individuals. In agreeing that both the speed and effectiveness of the implementation of program change control is a big risk, one CIO noted that when systems are changed, the fear is “*not that someone will steal lots of money, but ... that the company will not be as effective as it should be*” – especially in large, decentralized enterprises.

If systems are deemed compliant in year one but changes are not closely monitored, compliance could be lost. Therefore, change controls may become more of a focus for CIOs in year two. One CIO

cautioned that without close monitoring of changes, *“you will naturally fall out of compliance, and companies will need to exert positive influence and be proactive to ensure this does not happen.”*

Relationships evolving, but not with the audit committee

One CIO sees three dimensions to how IT interacts with the organization:

- **Accuracy and completeness:** Assuring the accuracy of financial statements
- **Internal controls:** Mitigating risk and meeting both internal and external audit requirements
- **Transparency and accessibility:** Providing information to the organization

Since IT is a key delivery system for financial reporting, enterprise-wide risk management, and Section 404 compliance, it is easy to see why the audit committee would be interested in the IT function. However, in our conversations with CIOs, we found that relationships with the audit committee have not evolved in recent years as much as one might expect, given areas of common interest and responsibility.

Board of directors: Becoming more IT savvy – but should technical expertise be required?

CIOs report that since the passage of the Sarbanes–Oxley Act in 2002, board members have begun to ask deeper questions in an effort to become better informed on issues related to IT. One CIO noted, *“they all probe and ask me what they want to.”* CIOs were mixed in their assessment of how much information the board has or needs. One view is that board members *“are familiar with IT, but it is not first or foremost [among their concerns].”* Another perspective is that *“before Sarbanes–Oxley, the board would never have asked about access control, and now they do.”*

One CIO questioned if boards have enough technical expertise to delve into the IT issues important to their companies; he stated, *“There is not enough knowledge on boards. Sarbanes–Oxley had a scramble to pull CFOs onto boards, but there should be a similar scramble to pull CIOs and IT individuals onto boards.”*

Audit committee: Interaction dependent on management reporting structure – a source of risk?

Very few CIOs have personal contact with the audit committee, and there appears to be a link between the company’s management reporting structure and the presence of a direct relationship between the CIO and the audit committee. Every CIO who reports directly to the chief executive officer presented directly to the audit committee. In contrast, if the CIO reports to the chief financial officer or to another individual within the company, direct contact with the audit committee was unlikely to occur.

With reporting structures apparently a driver of the relationships the audit committee develops, audit committee members may question whether they are gaining an appropriate level of insight. If the audit committee is working through an intermediary, is it missing an opportunity to gain insights into information directly from the CIO? To mitigate possible risks inherent in a blocked communication channel, audit chairs might find it worthwhile to initiate conversation with the CIO if a current relationship does not exist.

The lack of meetings with the audit committee was not a concern to one CIO, who noted that he does not currently meet with the board or the audit committee on any issues, but feels that *“they are aware of*

the issues.” However, there is an appetite among other CIOs without direct access to have more frequent interaction with the audit committee. One CIO mentioned he has not met with the audit committee in five years, since Y2K. He said, *“The audit committee chair is well-informed of the issues, but it wouldn’t hurt to sit down from time to time to share information.”*

One CIO anticipated a change that might occur in this relationship now that board directors are facing a greater risk of liability. He asked, *“Is the audit committee’s role changing to encompass more personal accountability? If so, they will need to go through more work to understand the detail and this will take more work from IT to provide information.”*

Internal audit: Still making time to assist IT – but do they have enough time to give?

CIOs reported a positive and symbiotic relationship with the internal auditors. One CIO noted, *“The relationship of IT with internal audit is one of ‘you scratch my back, I’ll scratch yours.’”*

Not only are most IT functions working closely with internal audit on Section 404 compliance work, the two groups also collaborate on implementing new business projects. The internal auditor provides critical input up front during IT systems design phases; describing the relationship, one CIO remarked, *“this way preventive controls are put in place, versus solving problems after the fact.”* Another CIO noted, *“Internal audit helps us to determine what we can do differently in our work and does not just validate controls.”*

CIOs indicated the interaction between internal audit and IT during the systems implementation phase has decreased due to internal audit’s significant Section 404 commitments. One CIO explained that although internal audit is less available this year, *“the two groups are still meeting, but less frequently or for shorter durations.”* Still, he did not think the meetings were so infrequent as to have hurt the company.

In the past, audit chairs have questioned if internal audit could have better relationships with other business functions if it was not so busy with Section 404. In a meeting of the Audit Committee Leadership Network, one audit committee chair asked, *“Section 404 has taken a tremendous amount of internal audit staff [time]. There is an opportunity cost. What is not being done? And what is the risk of that?”*³

External audit: Stronger relationships; increased understanding

As a result of Section 404 compliance work, CIOs also report a change in the nature of their interaction with external auditors, which they describe as having become more involved and intimate. As one CIO said, *“External auditors are exerting a stronger voice than [they did] in the past.”* Another remarked that because of Section 404, *“I have spent an ungodly amount of time with the external auditors in the past twelve months.”* CIOs said they appreciated the outside perspective that external auditors brought to the compliance efforts. On this point, one CIO said, *“they brought value to the process.”*

A large part of the benefit from the improved relationship between IT and the auditors has been in the process of determining how to work together to meet new requirements. One CIO said, *“they are learning in the process with us on interpretation of Sarbanes–Oxley, how to test, and how we can support them in their efforts.”* As another CIO noted, *“bonds have been strengthened and now there is*

³ Audit Committee Leadership Network, “Section 404: Lessons learned and value earned?” *ViewPoints*, June 4, 2004, 4.



stronger confidence in this relationship going forward... the external auditor knows us better and we have stronger processes.”

Finance/operations: Becoming more integrated

Recent regulatory changes have also proved beneficial to the IT department’s relationship with other business functions, most notably with finance and operations. CIOs mentioned that Section 404 helped to close the gap between the IT and finance departments because so much financial reporting is processed through IT systems. This positive outcome of Section 404 was most apparent in companies which proactively planned for an integration of IT and finance. One CIO said, *“This [improved relationship] was a by-product, but the efforts were organized to ensure it happened.”* Senior financial executives agree. Recent polling by *CFO-IT* magazine showed an unexpected positive outcome of Sarbanes-Oxley was improved relationships between finance and IT. Further, 95% of the 241 finance executives polled believe that relationships between IT and finance are essential or very important for business alignment.⁴

Big questions: What should the audit committee be asking the CIO?

One CIO thought it was important for the audit committee to, *“Ask the right questions and listen for the wrong answers. Listen for patterns, not single points of light. Audit chairs should not get hung up on single points of failure but need to find the root cause of the problem, to see if it is endemic of a larger issue. This root cause might be cultural.”*

To begin the dialogue, one CIO recommended the following series of questions: *“Have you talked to other CIOs in your industry? What are the big issues for your colleagues? Have you gathered a wide range of inputs from others outside of your company? On the issues, how does your organization stack up? Are you the forerunner, in the middle or the back of the pack?”*

⁴ Scott Leibs, “One Way or Another,” *CFO-IT*, Winter 2004, 21.



Big questions: what the audit committee should ask the CIO

Internal controls

- Once system controls are developed, how do you ensure they stay in place? What events could cause IT controls to fall out of compliance?
- How can IT help make Section 404 compliance more sustainable?

General IT controls: Access

- What have you done to ensure segregation of duties? How do you ensure that access rights change when people change jobs?
- How many people have sufficient access to significantly disrupt the company's network? What are the limits on their access?
- How do you ensure that mission-critical and/or sensitive information is protected?

General IT controls: Program development and change

- How confident are you that all software is documented and meets quality standards (and that backdoor entry points created during application development are closed)?

Crisis prevention and management

- What framework does IT use to assess actual risks, risk awareness, and risk prevention?
- How long could the company's systems be down in a crisis event before significant damage to the company was done?

Outsourcing

- Are all outsourced operations SAS 70 compliant?

Value creation

- How does IT contribute to shareholder value?
- What metrics do you use to evaluate your work? What other metrics should be used?

Conclusion

As companies become increasingly dependent on IT, audit chairs will need to forge closer relationships with CIOs to gain the insights necessary to perform their oversight duties. CIOs understand that audit committees are spending more time than ever on IT matters and welcome more interaction. The interaction is mutually beneficial: audit chairs can learn from the perspectives of CIOs, and CIOs can benefit from the insights they gain through meeting with the audit committee. Much in the same way that the audit committee and management help to set the “tone at the top,” CIOs play a large role in setting the right tone on compliance in their companies. By working with CIOs, audit committee chairs not only become aware of IT issues they might not otherwise see, they also have the opportunity to reinforce good governance practices.

InSights

FOR AUDIT COMMITTEE MEMBERS



About this document

InSights is produced by Tapestry Networks to provide assessments of key issues of interest to audit committees. Initially, *InSights* will be distributed to network members who, in turn, will share it with colleagues on audit committees and boards, and their advisers. It will be distributed by Ernst & Young to its partners. Anyone who receives *InSights* may share it with those in their own network. The ultimate value of *InSights* lies in its power to help all constituencies develop their own informed points of view.

The views expressed in this document represent those of the individuals who participated in the research. They do not reflect the views nor constitute the advice of network members, their companies, Ernst & Young, or Tapestry Networks. Please consult your counselors for specific advice. Ernst & Young refers to all members of the global Ernst & Young organization, including the U.S. member firm of Ernst & Young LLP.

This material is copyright Ernst & Young and prepared by Tapestry Networks. It may be reproduced and redistributed, but only in its entirety, including all copyright and trademark legends.