



INFOSCREEN

The Sarbanes-Oxley Act of 2002 (SOX) has far reaching implications for the governance of public US corporations. Spawned by a series of high profile business scandals, SOX was enacted to institute a system of checks and balances that improve corporate transparency and accountability. One of the most fundamental aspects of the legislation is its focus on internal controls over financial reporting and disclosure (Section 404).

The spirit of this emphasis on internal controls is straightforward enough. Management and financial auditors cannot attest to the accuracy of financial reports without sufficient confidence in the systems used to gather, transmit, store, manage, and analyze corporate data. Unfortunately, there is a broad gap between understanding the mindset of the SOX framers and assuring corporate stakeholders that an organization is sustainably SOX compliant. This is particularly true given the newness of the legislation and ambiguity around how forcefully the SEC will enforce it.

The Public Company Accounting Oversight Board (PCAOB) is chartered to assist both internal and external auditors in their SOX compliance work. PCAOB states:

Internal control is not “one-size-fits-all” and the nature and extent of controls that are necessary depend, to a great extent, on the size and complexity of the company. Large, complex, multi-national companies, for example, are likely to need extensive and sophisticated internal control systems.¹

In practice, prudent corporations will document their basis for determining the general scope of their internal controls and areas of special emphasis; a sort of Mission Statement for the on-going SOX compliance steering effort. For starters, this internal control structure should be based on industry best practice and a general recognition of the corporation’s scale and complexity. At the detail level, the right mix of controls should reflect an objective assessment of issues that can undermine accurate financial reporting. SOX clearly puts public corporations on notice, both large and small, that ignorance of material weaknesses in a corporate control environment will not appease the SEC.

2004 will be remembered as the year that corporate America raced to comply with SOX Section 404. 2005 offers an opportunity to slow down and take stock of the lessons learned. A variety of indirect benefits will certainly accrue to those corporations that can build upon the internal controls and culture of compliance spawned by this legislation.

¹ PCAOB, “Release No. 2004-001: An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements” p.9

The relationship between Section 404 internal controls and information security.

PCAOB does not address IT controls in any detail. That said, documented and auditable IT controls are certainly part of any compliant control environment.

IT controls may be viewed as a subset of information security controls in this context. At the very least, information security controls and internal controls over financial reporting are overlapping spheres of business practice. A complex organization cannot attest to the accuracy of any operational report in the absence of basic information security controls, such as sound passcode practices. Before SOX, management might turn a blind eye to passcode policy abuses, such as written passcodes in plain sight, passcode sharing, and IT staff vulnerability to social engineering exploits. In fact, senior managers are often the worst abusers, setting a poor example for rank and file employees. SOX is likely to change behaviors, as the Big 4 reports on IT control deficiencies as part of their attestation work.

One of the keys to implementing a sustainable SOX Section 404 compliance program is to understanding how IT systems can impact reliable financial reporting. By applying a structured approach to the internal assessment effort, the areas for potential problems can be framed out and resolved. For example, one InfoScreen client recognized segregation of duties as a critical area for improvement. The outcome was tighter security controls in SAP to disallow, for example, one user from creating a vendor and generating an invoice. It takes careful thought, informed by an intimate understanding of the business, to devise an effective IT control environment that thwarts careless actions and fraud alike.

Mark Slicer, an Executive member of the General Electric audit staff who was recruited from PWC in late 2003 for a leadership role in the corporation's SOX compliance effort, notes that many of the process improvements at GE have reflected the complexity of IT's relationship to Finance. He observes that GE's decision to start the internal Assessment process in 2003 created opportunities for lessons to be learned, providing a clearer path for certification in 2004.² A check box orientation will not deliver the sustained culture of compliance mandated by the legislation. A rigorous internal assessment followed by remediation work and associated documentation takes time.

Late 2004 has seen an almost frenetic scramble by corporations, consultants, and auditors to comply with SOX. Much of this work has concentrated on IT controls associated with financial systems. InfoScreen anticipates that many smaller corporations will fail to receive 404 certification due to IT related issues and many more will find that their Audit Committee has been put on notice of deficiencies in their IT controls. 2005 will be a time to step back and sift through the lessons learned. Prudent companies will build on these efforts to document a passable IT control environment and establish long term business practices that deliver benefits beyond a clean auditor opinion.

² Mark Slicer, GE Audit Staff Executive Financial Advisor. Presentation at Cornell University. November 2, 2004.

Industry standards

PCAOB recommends the Committee of Sponsoring Organizations (COSO) framework for defining, implementing, and managing the appropriate internal control structure.³ While SOX does not reference COSO and PCAOB does not mandate COSO, this does appear to be the safest general framework for structuring a SOX compliant internal control environment.

Control Objectives for Information and related Technology (COBIT)⁴ appears to be the emerging standard for information security best practice, driven in large part by the financial audit community's longstanding ties to COBIT's authoring organization. InfoScreen has been applying the International Organization for Standardization (ISO) 17799⁵ framework since 2001, reflecting our manufacturing sector focus. Given the more recent preeminence of COBIT, we now apply a hybrid framework based on both COBIT and ISO.

Implications for small to medium sized public corporations

While SOX has been called a knee jerk reaction to the turn of the millennium wave of corporate scandals, all indications suggest that SOX is here to stay.

SOX compliance undoubtedly costs time and money. Despite the no one-size-fits-all caveat, small public companies are disproportionately burdened, particularly where their revenue stream includes complex financial transactions. For example, in any case, regardless of the corporation's size, where inaccuracy in a class of complex financial transactions can have a material impact on consolidated financial reporting, an auditor will be expected to perform walk-throughs to evaluate the process flow and reliability of typical financial transactions⁶ Management's inability to provide evidence of an effective IT control environment, including careful documentation and sufficient monitoring, represents a material weakness - obligating an auditor to release an adverse opinion or at the very least to disclaim an opinion.

Pundits observe that SOX will stimulate a trend among smaller public companies to take themselves private, motivated in large part by alleviation of the growing burdens of compliance.

³ www.coso.org

⁴ www.isaca.org/cobit

⁵ www.iso.org

⁶ PCAOB, "Auditing Standard No. 2 – Internal Control. Staff Questions and Answers, Auditing Internal Control Over Financial Reporting" Question 28. October 6, 2004.

In a recent congressional hearing, PCAOB Chairman William McDonough stated “ A small or medium size company simply does not need the bells and whistles on internal controls that General Electric needs. It would be very ill-advised and a terrible waste of money for them to have all those bells and whistles. So we expect them to look at the nature of their business, how complicated it is, how difficult are the internal controls, to make sure that they have the level of internal control that they really need.”⁷ With the recent boost in President Bush’s political capital, and comments such as Chairman McDonough’s, it is tempting for smaller public companies to anticipate some relief moving forward.

McDonough’s comment sounds generous on the surface, but reveals its teeth on closer inspection. In practice, 404 certification means having the internal controls that are really needed. No more, but probably no less.

Moody’s has offered some useful guidance on how material weakness disclosure will impact the corporation. The Moody’s position paper acknowledges the scramble for SOX compliance and the fact that many corporations have underestimated the task. The significance of any disclosed weaknesses must be judged in terms of their seriousness and management’s response. Moody’s plans to give companies that show “Category A” weaknesses (weaknesses that can be audited around) “the benefit of the doubt” and will not take any rating action.⁸ InfoScreen does not anticipate similar leniency in 2005.

Many detail level COBIT/ISO controls may be overkill for smaller manufacturers. In a recent release from the IT Governance Institute, the esteemed group of 51 authors and reviewers acknowledge the need for business context, observing for example “if systems development is considered to be of low risk, an organization may choose to amend or delete some of the suggested detailed control objectives.”⁹ An informed and proactive approach helps management stay ahead of the SOX curve without excessive investment or the introduction of unnecessary controls that can undermine productivity.

⁷ US Representative Richard Baker (R-LA) Holds a Hearing on Public Company Accounting Board Oversight – Committee Hearing Transcript. June 24, 2004.

⁸ Moody’s Special Comment “Section 404 Reports on Internal Control: Impact on Ratings will Depend on Nature of Weaknesses Reported”. October 2004.

⁹ IT Governance Institute “IT Control Objectives for Sarbanes-Oxley. The Importance of IT in the Design, Implementation and Sustainability of Internal Control Over Disclosure and Financial Reporting”. April 2004

At a recent Financial Executives International (FEI) meeting, a panel of smaller corporation executives offered useful perspective on senior management's role in the SOX process. One of the outcomes of the SOX emphasis on auditor independence is that many corporations are looking to a major accounting firm that is not their financial auditor of record for SOX compliance consulting. In the scramble for certification, many of these consulting engagements have not gone so smoothly, as the Big 4's 'A team' resources have been allocated to larger clients. The onus falls on senior management to own the 404 process.¹⁰

The broader benefits of SOX compliance

It is straightforward enough to imagine ways in which poor IT controls and other information security controls can lead to inaccurate financial reporting. For example, a disgruntled employee might tamper with a back office system to create a false picture of bookings or inventory. Corporations need methods for identifying unauthorized entries and other affronts to accuracy, along with evidence that they are actually using these tools and periodically testing their effectiveness. In order to keep pace with SOX interpretation, smaller public manufacturers at the very least need basic information security as part of their foundation for accurate financial reporting.

The benefits of sound information practice extend much further. As noted previously, IT controls can be viewed as a subset of information security controls. SOX means that responsibility for IT controls can no longer sit squarely on the shoulders of IT management. SOX also motivates corporations to abandon a functional approach to information security, where IT, HR, Legal, Facilities, Engineering, Operations, etc. don't collaborate enough.

For example, a corporation that recognizes a competitive advantage in its high level of employee morale and a business culture of broad employee participation, should maintain effective controls around careless employee disclosure. While there may be other checks and balances in place to prevent a link between careless disclosure and inaccurate financial reporting, the damage to competitive positioning may persist. Similarly, there may be other internal controls over financial reporting to prevent a link between, say physical security gaps or weak HR practices, and inaccurate financial reporting. SEC disclosures may be accurate, while hard earned intellectual property remains vulnerable to both malicious and inadvertent loss.

¹⁰ Financial Executives International (FEI), Current Financial Reporting Issues Conference. November 2004.

The SOX compliance requirement creates opportunities to improve a corporation's broader control over sensitive information, as well as the security of people and physical assets. SOX requires internal controls over financial reporting and disclosure. Smart companies will build upon this control structure to reduce more generalized operational risks and improve assurance of their future competitiveness. Loose lips can sink ships. A Human Firewall where employees understand their roles and responsibilities around Need to Know and the reporting of suspicious events can help a company to soar.

SOX compliance may also yield commercial benefits. While it is not yet possible to obtain an ISO stamp for information security best practice, using ISO 17799 as the model probably affords the most direct link between information security and business development. This is particularly true for manufacturers that routinely interface with proprietary customer information, where a demonstrated commitment to information security best practice will put customer concerns at ease. A customer that must share its own proprietary information with certain vendors is more likely to partner with the supplier that takes information security seriously. The InfoScreen approach affords companies the commercial benefit of ISO while also appeasing financial auditors and the SEC by applying COBIT.

The InfoScreen approach

InfoScreen applies a 3 phase approach to helping companies maintain SOX compliant IT controls over financial reporting, as well as a balanced set of controls over sensitive company information.

InfoScreen's manufacturing sector focus, and experience working with mid sized manufacturers, informs our guidance when consulting on effective IT controls. InfoScreen spun off from Clarity Consulting, Inc. (www.claritydelivers.com) in 2002 and retains ties to this industrial and high tech market research and consulting firm – providing additional context. Clarity works almost exclusively for large Diversified Industrials, including ABB, Alcan, Dover, Eaton, and Emerson. InfoScreen targets smaller manufacturers.

InfoScreen's background enables us to apply a pragmatic approach to the control refinement process, basing our guidance on the client's actual business activities and real world threats to information integrity along with current opinion from PCAOB and both the financial and IT audit communities. We endeavor to help manufacturers to stay one step ahead of the SOX requirements while deriving additional benefits from these mandated controls.

In Phase 1, InfoScreen performs a thorough Assessment of the current state. This assessment reflects both the SOX emphasis on potential material weaknesses in IT controls over financial reporting, as well as an integrated COBIT and ISO 17799 emphasis on threats to corporate information. InfoScreen maintains a pragmatic and non-emotional orientation, purging Fear Uncertainty and Dread (FUD) from the process and concentrating on real world fraud and loss scenarios. One of InfoScreen's key differentiators is our focus on social or human risk factors. We understand the pitfalls of disproportionate investment in network security without commensurate attention to the ways that people, (insiders and 3rd parties, malicious parties and careless actors alike) put corporate information at risk.

In Phase 2, we work with management to apply the Assessment findings toward the development of appropriate process improvements and documentation for SOX compliant IT controls and more broadly defined information security controls. We consider the relevance of certain controls as they pertain to the client's business model and likely threats to intellectual property and accurate financial reporting. Depending on the scope of engagement, we can expand upon the protection objectives to include physical assets and people. We understand that overly stringent controls undermine productivity and increase operational costs without sufficient offsetting risk mitigation.

Clearly, there are differences between a SOX compliant set of IT controls and a balanced set of information security controls. That said, there are more than enough commonalities between these two control systems to justify an integrated process for both activities. In a recent release from the IT Governance Institute, the authors map COSO against COBIT. The output is a rewritten set of 136 control objectives distilled from the broader set of 318 COBIT controls objectives. This guidance is presented as an IT controls framework for SOX compliance.¹¹ InfoScreen addresses the IT facet of SOX while supporting the broader SOX steering effort and advancing the general security of intellectual property.

In Phase 3, InfoScreen performs period audits to evaluate organizational compliance with the controls defined and implemented in Phase 2. We encourage internal resources to shadow our audit work and facilitate the transfer of responsibility for certain audit activities to internal resources.

¹¹ IT Governance Institute "IT Control Objectives for Sarbanes-Oxley. The Importance of IT in the Design, Implementation and Sustainability of Internal Control Over Disclosure and Financial Reporting". April 2004.

Our work to integrate the COSO framework for reliable financial reporting, along with COBIT and ISO 17799 for information security practices, means maximum value for InfoScreen clients. Our approach reflects careful guidance from the financial and IT audit communities. We stand behind the opinion that our approach will satisfy accounting firms and SEC auditors alike because the outcome of our work is so directly tied to good business practice. To the greatest extent allowed, we collaborate with your financial audit firm to confirm that the IT controls in place are satisfactory. We are also comfortable participating in the refinement of non IT specific internal controls over financial reporting and disclosure. Auditors want to see evidence of careful threat analysis in the creation of a documented internal control structure, along with evidence that operations are compliant with these controls. Auditors are not so much in the business of evaluating the efficacy of these controls themselves, but rather confirming the existence of carefully devised controls over financial systems that are actually used. If SOX means that organization must go to these lengths, InfoScreen helps assure management that the new control structure also delivers real improvements to the security of hard earned corporate assets.

Contact

Rich Sheiman, President
InfoScreen, Inc.
401 East State Street – Suite 400
Ithaca, NY 14850
(800) 613-1925 Extension 212
sheiman@infoscreen.com