books24x7 a SkillSoft Company

ExecBlueprints™

in partnership with Aspatore Books

Action Points

I. **Breaking Down Sarbanes-Oxley Compliance**
Sarbanes-Oxley is no longer just for public companies. Companies are now requiring their vendors to conform to compliance standards, and other companies are recognizing the benefits of compliance on their systems and infrastructures. Sarbanes-Oxley is not just about compliance – it's about objective standards that require structural integrity and increase efficiency.

II. **The Bottom Line – Monitoring Impact**
The successful implementation of Sarbanes-Oxley will be visible in its impact on control systems' stability and cost savings.

III. **Must-Haves for Ensuring Successful Compliance**
Create relationships. Look at certification programs. Strike a balance. Test and retest. Consider compliance an enterprise-wide effort, requiring collaboration and creative strategizing.

IV. **The Golden Rules for IT's Involvement and Support**
Technology alone is not the answer: people are. IT personnel should investigate ways technology can automate and standardize processes in all areas of the company.

V. **Essential Take-Aways**
An international company has another set of challenges as they attempt to comply to U.S. standards and possibly international standards also. Our authors give tips on how to handle this challenge.

Contents

About the Authors p.2
Kelly L. Frey p.3
Francis X. Taney p.7
Robert Wucher p.10
Ideas to Build Upon & Action Points . . . p.13

Three top technology experts from Baker, Donelson, Bearman, Caldwell & Berkowitz, Buchanan Ingersoll & Rooney, and Wucher and Associates share their insights on:

The Top Five Tips Every Technology Executive Needs to Know About Sarbanes-Oxley

Kelly L. Frey, Sr., MS, JD
Shareholder
Baker, Donelson, Bearman, Caldwell & Berkowitz PC

Francis X. Taney, Jr.
Shareholder, Buchanan Ingersoll & Rooney PC

Robert Wucher
Principal, Wucher and Associates

Companies are realizing that Sarbanes-Oxley is not just about compliance — it's about increasing efficiency, using objective standards to create an infrastructure and track transactions and processes, and ultimately, saving the company money. Our authors discuss their tips for understanding compliance, monitoring its implementation and impact, best practices for ensuring successful compliance, and IT's role. They also look to the future and the industry standards they believe will be coming soon. Ultimately, this EB will help explain what Sarbanes-Oxley can mean to your company — and how its effective implementation can increase efficiencies and save costs with a visible effect on the bottom line. ■

About the Authors

BAKER DONELSON
BEARMAN, CALDWELL & BERKOWITZ, PC

Kelly L. Frey, Sr., MS, JD

Shareholder, Baker, Donelson, Bearman, Caldwell & Berkowitz PC

Kelly Frey is a shareholder in Baker Donelson's Nashville office and a member of the firm's business law department. He concentrates his practice in the area of corporate and information technology law. He represents the headquarters locations of several Fortune 500 companies in both procuring and selling information technology. Additionally, he represents large companies and the vendors to such companies with respect to general corporate transactions and corporate compliance.

Mr. Frey has extensive experience in negotiating and drafting confidentiality agreements, term sheets, letters of intent/memoranda of understanding, software development and licensing agreements, business process and IT outsourcing agreements, ASP agreements, consulting agreements, and content licensing agreements (for both traditional and new media). He has been involved in all phases of corporate procurement, including development of RFPs and evaluation of vendor proposals on the purchaser side, preparation of responses to such RFPs on the vendor side, and negotiation/drafting of final contract documentation. He also consults with vendors to regulate companies with respect to new compliance requirements resulting from The Sarbanes-Oxley Act, Gramm-Leach-Bliley, Health Insurance Portability and Accountability Act, USA PATRIOT ACT, OFAC, EU directives, and other compliance environments.

Mr. Frey also regularly advises clients on intellectual property matters (including copyright, trademark, trade secret, domain name, Internet, and e-commerce issues) and serves as the primary legal resource for new business ventures in the information technology industry. As a result of his emphasis on helping clients achieve their practical business goals and his integration within the operations of his clients, Mr. Frey has been named as co-inventor on numerous business process patent applications filed by his clients.

☛ *Read Kelly's insights on Page 3*

Francis X. Taney, Jr.

Shareholder, Buchanan Ingersoll & Rooney PC

Frank Taney chairs the information technology litigation practice group and is a member of the technology transactions group.

He has successfully tried many arbitrations and bench and jury trials to award or verdict as lead trial attorney, and has other trial and arbitration experience. In addition to his IT litigation practice, Mr. Taney has negotiated IT-related transactions for a number of his clients, including software licensing agreements, IT outsourcing, Web hosting, software development, and other IT service contracts. He has also counseled clients on methods to avoid or minimize the adverse impact of IT-related disputes.

Mr. Taney is a frequent lecturer and author on topics relating to information technology law, litigation, and related transactions. He regularly conducts public seminars for attorneys and business executives on IT-related legal topics.

Mr. Taney has been published and quoted on IT-related topics in publications such as *InformationWeek*, *Technology Times*, *Computer World*, *IT Professional*, and *SmartBusiness Philadelphia*. Mr. Taney has also provided formal and informal private instruction on IT-related legal topics to business executives and in-house legal staff for a number of private and publicly traded companies. He contributed the chapter "Navigating the IT outsourcing and procurement process" to a book from Harris Kern's Enterprise Computing Institute titled *CIO Wisdom II: More Best Practices*.

In 2005, 2006, and 2007, Mr. Taney was named as a Pennsylvania Rising Star in *Philadelphia Magazine*. He has also been included in the 2006 to 2007 edition of Marquis' *Who's Who in America*, and the 2007 to 2008 edition of *Who's Who in American Law*.

☛ *Read Francis' insights on Page 7*

Robert Wucher

Principal, Wucher and Associates

Robert Wucher has over 25 years of experience in the field of information technology (IT) at the senior and executive management level. He has worked extensively with government agencies, private organizations, and public companies. Industry experience includes the public sector, banking, manufacturing, Internet, health care, and not-for-profit organizations.

Mr. Wucher's areas of experience includes Sarbanes-Oxley (Section 404) IT Compliance and Auditing, Systems Auditing And Controls Review (SAS-94, SAS-70), Forensic Data Analysis and Auditing, Information Technology Strategic Planning, Systems Selection And Request-For-Proposal (RFP) Development, Project Management, Systems Development And Implementation, Systems Programming and Data Conversion, Systems and Data Integration, Disaster Recovery Planning, and e-Commerce And EDI Systems.

Mr. Wucher belongs to the volunteer and mentor program at Larkin Street Youth Center, and is a former board member of Pets are Wonderful Support (PAWS). He is also a MAS-90 Accounting Application Suite Qualified Installer, SAGE Systems.

He has a B.S. in business administration from Old Dominion University.

☛ *Read Robert's insights on Page 10*

Kelly L. Frey, Sr., MS, JD

Shareholder, Baker, Donelson, Bearman, Caldwell & Berkowitz PC

SOX compliance has actually yielded positive results for many corporations, creating cost savings in larger companies. These cost savings range from elimination of redundant systems to implementation of uniform data structures and automation of previously manual control systems.

Kelly L. Frey, Sr., MS, JD
Shareholder
Baker, Donelson, Bearman, Caldwell & Berkowitz PC

Breaking Down Sarbanes-Oxley

Most importantly, executives should be aware that SOX is not solely for public companies anymore. Most SOX-regulated companies are now forcing their technology vendors to conform to the customer's SOX compliance standards via their technology contracts.

Secondly, SOX is not strictly about compliance; rather, it is about articulating an objective standard for the integrity of information within an organization. Technology executives should also be aware that SOX uses many different frameworks and schemas, but there is substantial similarity and overlap between them. Most non-SOX-regulated companies are familiar with a SAS Type II audit. However, that type of audit merely certifies that control processes are in place and functioning, and that they are auditable over a six month time period. They are not prescriptive with respect to exactly what controls are in place. The result is that every potential vendor can have a different control process, all of which are capable of passing a SAS audit.

Another item about which executives should be aware is that standard industry certifications will be coming soon. The ISO 17799[1] standard is rapidly replacing the many customized control systems that are in place in non-SOX-regulated companies. ISO 17799 is a comprehensive set of controls comprising best practices in information security. The standard comprises 10 prime sections: security policy, system access control, computer and operations management, system development maintenance, physical and environmental security, compliance, personnel security, security organization, asset classification and control, and business continuity management.

Finally, SOX compliance has actually yielded positive results for many corporations, creating cost savings in larger companies. These cost savings range from elimination of redundant systems to implementation of uniform data structures and automation of previously manual control systems.

The Impact of SOX on the IT Department

Any time SOX is mentioned, it is important for executives and employees alike to think in terms of "cost savings," not just cost. Information technology personnel should consider how automating and standardizing data collection and reporting can reduce expenses

1. See generally, http://www.iso-17799.com/.

Kelly L. Frey, Sr., MS, JD
Shareholder
Baker, Donelson, Bearman, Caldwell & Berkowitz PC

"Technology can assist in compliance and the metrics used to describe compliance, but technology alone is not the answer. People are the answer."

- *Has extensive experience in negotiating and drafting confidentiality agreements, term sheets, letters of intent/memoranda of understanding, software development and licensing agreements, business process and IT outsourcing agreements, ASP agreements, consulting agreements, and content licensing agreements (for both traditional and new media)*
- *Consults with vendors to regulated companies with respect to new compliance requirements resulting from The Sarbanes-Oxley Act, Gramm-Leach-Bliley, Health Insurance Portability and Accountability Act, USA PATRIOT ACT, OFAC, EU directives, and other compliance environments*
- *Named as co-inventor on numerous business process patent applications filed by his clients*

Mr. Frey can be e-mailed at kelly.frey@execblueprints.com

across the enterprise. They should look at how standardization — using any of the SOX-compliant standards — can create efficiencies in operations and result in better financial controls and reporting.

In many ways, SOX compliance is the new "year 2000" problem for information professionals in all companies. IT professionals can either be resistant and view this as a cost element or they can embrace the opportunity to utilize the regulatory requirements to create better, more efficient internal architecture for their companies.

The biggest misconception most CTOs and executives have about Sarbanes-Oxley is that SOX rules are for the benefit of investors and the senior management of the company (and not for the company as a whole). While the rules are designed to create accountability to shareholders by senior management, their implementation is really a matter of creating an auditable, enterprise-wide system for processing and reporting transactions, and this will ultimately benefit all involved.

Monitoring SOX Changes and their Impact

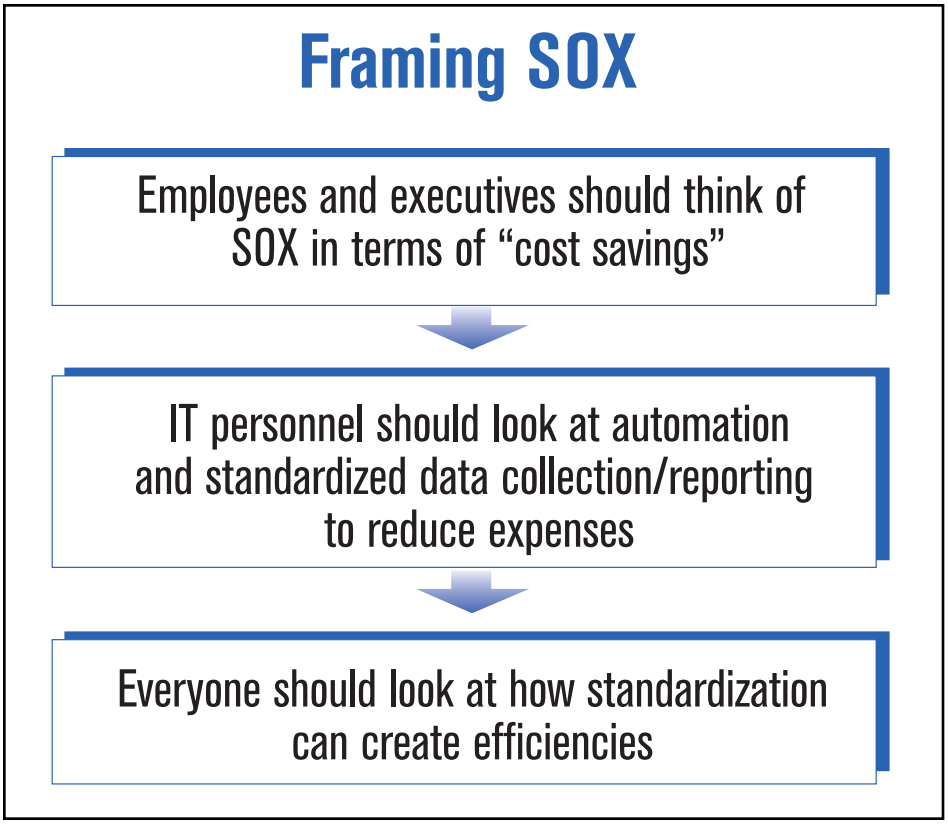
In order to obtain accurate and insightful information about the law and its basic requirements, CTOs should look to the standards organizations rather than only their legal compliance experts. This is because it is at the standards level that actual implementation occurs. For example, ISO 17799 and COBIT are specific standards that specify technical standards consistent with the reporting requirements for SOX. There are also certification programs that will benefit CTOs in better understanding the compliance schema and how to implement them; the Certified Information Systems Security Professional (CISSP) program is one example of such a program.[2]

CTOs can monitor changes by looking to standards organizations. The information they would receive from "legal" would pertain to what is needed at a conceptual level, but they would not receive a lot of direction on how things needs to be executed on a practical level to be in compliance.

Best Practices to Enhance an IT Department's Compliance Program

I recommend that IT personnel look at the certification requirements for the CISSP. That program identifies 10 different domains of expertise that must be mastered in order to cover the security and privacy concerns of a company adequately and, incidentally, cover much of the SOX-related process issues. The techniques do not require creative technology per se, but they do require creative problem solvers.

Other departments contribute to the success of these practices as well. Compliance and IT must work together. In fact, the largest increase in spending and headcount over the last couple of years has been in compliance departments. Each has a role and they need to be respectful of each others' role. However, they also each have unique contributions to make to the success of the company. Leaders are those that can synthesize and integrate concepts across compliance and IT. This is neither a "legal problem" nor a "technology problem;" rather, it is a problem



2. See generally, https://www.isc2.org/cgi-bin/content.cgi?category=97.

A technology executive will know if the firm is scoring well by looking at SAS 70 Type II, which is a "pass/fail" mark. As an analogy, when I think back upon my academic career, I remember taking a few pass/fail courses, but I feel strongly that the best courses were ones in which I expended more than the bare minimum effort to pass. Therefore, beyond the basic numbers, a technology executive will truly know when the firm is scoring well when stable control systems return auditable results that create cost savings for the company.

Kelly L. Frey, Sr., MS, JD
Shareholder
Baker, Donelson, Bearman, Caldwell & Berkowitz PC

requiring collaborative and creative strategies to build a framework and infrastructure that is not only sufficient for legal compliance but necessary for enterprise-wide efficiencies.

Benchmarks Used to Measure SOX Compliance

A SAS 70 Type II audit has historically been the benchmark that SOX-reporting companies have pushed out to their technology vendors via contract. However, that standard can be achieved with any number of proprietary systems. And the "Type II" designation merely reflects consistency of the system over the test period, which is typically six months. However, what most large companies want from a vendor is a commitment to operate within guidelines that are stable over a period of years and are standard across their industry. It is cold comfort to most Fortune 500 companies that a vendor can maintain a control system for six months. That is where the ISO 17799 standard and other comparable schemas come into play.

A technology executive will know if the firm is scoring well by looking at SAS 70 Type II, which is a "pass/fail" mark. As an analogy, when I think back upon my academic career, I remember taking a few pass/fail courses, but I feel strongly that the best courses were ones in which I expended more than the bare minimum effort to pass. Therefore, beyond the basic numbers, a technology executive will truly know when the firm is scoring well when stable control systems return auditable results that create cost savings for the company.

Simple audits of control structures can reveal whether financial transactions are consistent with financial audit standards at a level that allows a senior executive to certify to the financial standards accuracy and completeness. One test is by financial auditors: they determine whether or not the books add up and if it is possible to consistently replicate financial transactions down to the most elemental level. Again, it is important to remember that compliance is so much more than transactions, so it should be considered as part of a broader picture and not reduced to simple numbers.

Companies also have to be concerned about implementation of policies and procedures. For example, a company may have a well-defined policy related to physical security. However, implementation of that policy may require more than just publication of a policy manual. Simple metrics need to be in place to confirm that policies are actually implemented into everyday practice within the company. A company needs to continually monitor simple metrics in this regard and question their implementation of the policies for effectiveness. Does the company have a physical security program in place that assures that only qualified personnel have access to specific information? Is that security program auditable (via key card access, for example)? Are there practical controls in place to prevent "drafting" by non-qualified personnel (the classic example being a qualified person using a key-card to open a locked door, then holding the door open as a courtesy to a non-qualified person)?

The Role of Technology in the Measurement Process

IT departments have traditionally been the "gate keepers" since these

departments regulated automated systems and access to them. Now IT professionals are being called upon to be the "police" in that they have the unique position to monitor actual compliance, across the enterprise. Technology can assist in compliance and the metrics used to describe compliance, but technology alone is not the answer. People are the answer. Technology personnel have to be the voice of reason within the company, assisting in implementing technology but also integrating technology with the physical, financial, and corporate control processes that are required.

Calculating ROI for SOX Compliance

Calculating ROI on SOX compliance is a hopeless exercise. How do you quantify the worth of not having SEC regulators on site or the value of avoiding a senior management official being the subject of a civil or criminal charge? SOX is an absolute requirement of public companies, regardless of ROI.

ROI truly needs to be measured against the cost-savings inherent in creating an integrated infrastructure across the organization. How does one ever calculate the impact that a standard data-structure can have for a company? Certainly there is a cost savings when multiple systems can use the same database and structure across the company, and there are also savings with respect to not having to audit and reconcile different results from segregated databases; yet the true return on investment is at the enterprise level. This is revealed by the efficiencies gained when the entire organization can depend upon a single standard for data integrity and reporting.

To ensure the greatest ROI, there also should be a considerable percentage of a technology executive's time devoted to SOX compliance. Most larger companies have a chief compliance officer (CCO), which indicates that a substantial amount of time and resources are being devoted to compliance in general.

Challenges Faced by Global Firms

Global firms do face certain challenges with which domestic-only corporations do not deal. One such issue is exposure to regulatory environments that are not consistent with U.S. standards. For example, the E.U. has specific data privacy and security constraints that are not currently codified in the U.S. Companies wishing to share personal data across E.U. borders must either comply with the E.U. standards or seek the Safe Harbor provisions of the E.U. directive.[3] ■

3. See generally, http://www.export.gov/safeharbor/sh_overview.html

Francis X. Taney, Jr.

Shareholder, Buchanan Ingersoll & Rooney PC

The Secret to Complying with Section 404

While section 404 of the Sarbanes-Oxley Act has generated considerable attention and concern, and rightly so, I believe that at the bottom, section 404 imposes basic information security best practices on affected companies. Under the current state of the law and industry practice, information security means protecting the integrity, accuracy, confidentiality, and authenticity of data and related information systems and systems components. If a company accomplishes this, that company will have gone a long way; if not all of the way, toward ensuring a company's ability to comply with section 404. Therefore, in view, practicing sound information security is the secret to complying with section 404.

Concrete Steps Toward Effective Information Security and Section 404 Compliance

In general terms, information security is a fairly straightforward concept. A company must ensure that no one can prevent its employees and other authorized individuals from having appropriate access to protected information, systems, and systems components. Furthermore, one must ensure that no one has unauthorized access to these items, and that no one can modify, delete or falsify protected information.

The first key step toward achieving a compliant level of information security in general and for section 404 purposes is to perform an information security assessment. The assessment must be enterprise-wide, encompass both information and affected systems, and performed by someone with recognized information security certifications and credentials. The assessment should identify the material internal and external security risks and the potential harm that they pose, and match them up to the current security measures in place. After performing this matching, the assessment should determine the sufficiency of the current security measures in light of the nature and scope of the company's operation and the sensitivity of the information to be protected.

Once a company completes the initial risk assessment, the company should set about constructing and implementing a comprehensive information security program. This plan should be enterprise-wide, in writing, and authored and overseen by personnel with wide policy. The policy must be overseen and conducted by appropriately credentialed individuals.

Beyond this, the program should have appropriate technical, administrative, and physical security measures. Technical measures refer to technical security measures such as firewalls, intrusion detection software, anti-virus software, and the like. Administrative measures are procedural information security measures, such as employee training and education, or procedures and protocols for determining which employees have access to certain categories of information, and procedures for maintaining and changing passwords. Physical

In approaching information security and section 404 compliance, a company will have to strike a balance between security and controls and operational efficiency.

Francis X. Taney, Jr.
Shareholder
Buchanan Ingersoll & Rooney PC

Francis X. Taney, Jr.
Shareholder
Buchanan Ingersoll & Rooney PC

"Employing an interdepartmental and multidisciplinary approach gives a company the best chance of arriving at a lean but nevertheless section 404-compliant security and control structure."

- *Negotiated IT-related transactions for a number of clients, including software licensing agreements, IT outsourcing, Web hosting, software development, and other IT service contracts*
- *Frequent lecturer and author on topics relating to information technology law, litigation, and related transactions*
- *Named a Pennsylvania Rising Star in* Philadelphia Magazine

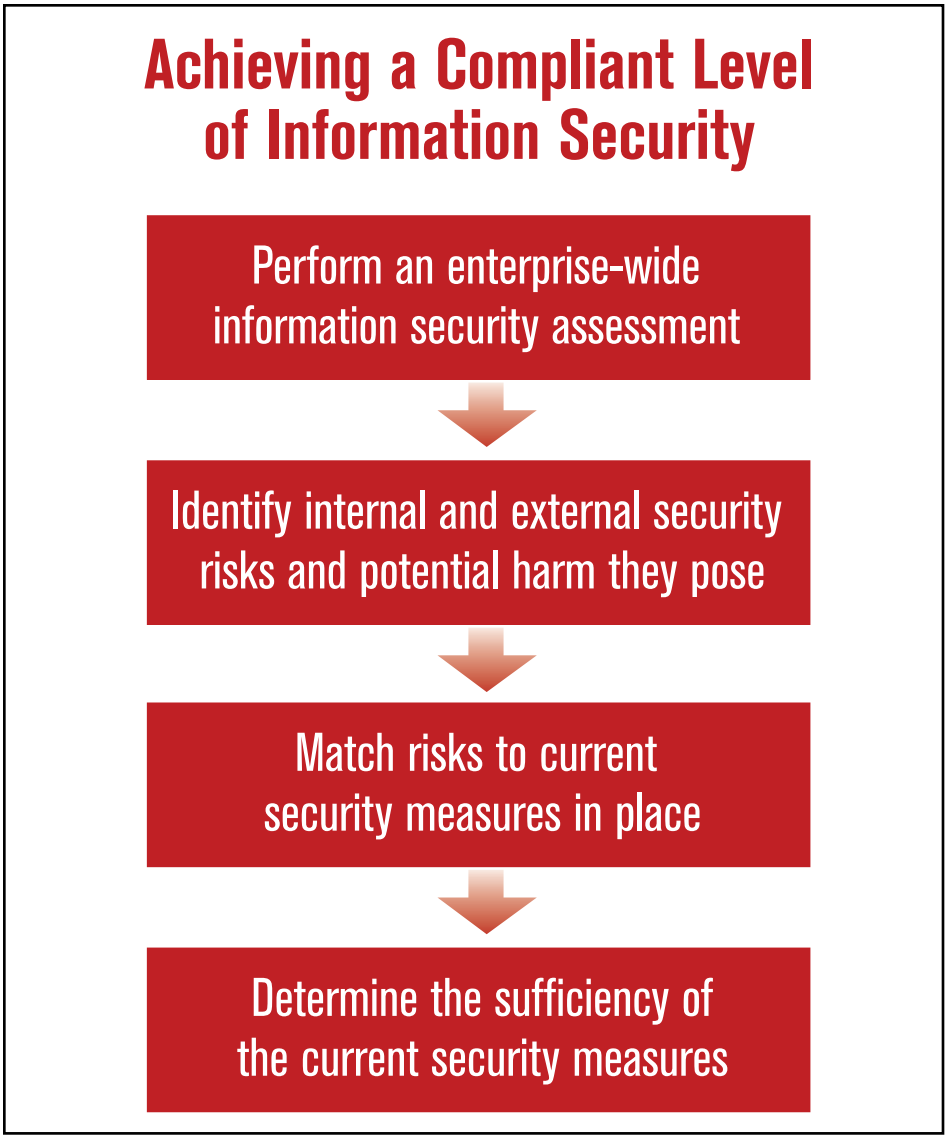
Mr. Taney can be e-mailed at francis.taney@execblueprints.com

security measures include features ranging from high to low-tech, such as key cards, biometrics, locked doors, closed-circuit televisions, security guards, and fences.

Upon putting the above security measures into effect, a company must monitor the operation of the security plan to ensure that the procedures are effectively carried out. Furthermore, the company should subject itself to independent third-party audits in order to "test the testers." Of course, when allowing any third-party organization to have access to company data or systems, a contractual agreement must be reached to ensure that they abide by the organization's security plan. It is also prudent as a matter of general policy to specifically and contractually require compliance with industry-specific regulations applicable to your company or your vendors.

Striking the Balance Between Compliance and Efficiency

In approaching information security and section 404 compliance, a



In approaching information security and section 404 compliance, a company will have to strike a balance between security and controls and operational efficiency. The IT function within a company could attempt to impose draconian security measures that, while effective in maintaining control and security, would grind the company's operations to a halt. This is obviously not the right solution. Neither is spending large amounts for the most bleeding edge gadgetry if the gadgetry is not necessary or adopted by the rank and file employees. Gadgetry that reduces costs and eases compliance by automating compliance functions, however, has a better chance of gaining acceptance and adoption.

Francis X. Taney, Jr.
Shareholder, Buchanan Ingersoll & Rooney PC

company will have to strike a balance between security and controls and operational efficiency. The IT function within a company could attempt to impose draconian security measures that, while effective in maintaining control and security, would grind the company's operations to a halt. This is obviously not the right solution. Neither is spending large amounts for the most bleeding edge gadgetry if the gadgetry is not necessary or adopted by the rank and file employees. Gadgetry that reduces costs and eases compliance by automating compliance functions, however, has a better chance of gaining acceptance and adoption.

In light of this need for balance, the IT function is just one leg of the tripod when it comes to developing an effective section 404 compliance strategy. IT must work with the legal department and the business people in order to flesh out the business and operational needs of the company. Legal can and must help this process by defining the scope or extent of the company's obligations with respect to how information is generated, maintained, stored, and manipulated. In turn, business and IT can help inform IT as to the prevailing standard of practice in the industry to help legal assess what the likely standard would be in the event of a problem involving the company's procedures and controls. Employing an interdepartmental and multidisciplinary approach gives a company the best chance of arriving at a lean but nevertheless section 404-compliant security and control structure. ■

Robert Wucher

Principal, Wucher and Associates

IT and the Auditing Process

It is hard to remember a time when information technology (IT) was not part of a company's financial audit process. In the past, the IT function was only interviewed to obtain an understanding of the financial systems environment in order to effectively plan and perform an audit (known as SAS-48, 55 and 94). Under Sarbanes-Oxley (SOX) regulations, activities are not only performed to document an understanding of the IT environment, but the key IT controls must be identified and validated through independent testing.

There are five tips one should consider when working under Sarbanes-Oxley compliance in an IT environment to avoid making common and sometimes costly mistakes. These include:

Tip One: Information technology controls are much broader and farther reaching than just those seemingly isolated activities performed in an IT department.

Many smaller and mid-sized companies will find their IT function is more of a network services group, which may also have some limited responsibility for maintaining a Web site, rather than a traditional IT department. As package-based applications and application service providers (ASP) have become more dominate, there are fewer IT departments that maintain programming and associated systems development staff. These roles have expanded outside of IT into service provider organizations and other departments such as sales and marketing, which often is responsible for the company's Web site, or finance and accounting, which maintains a large collection of supplemental electronic spreadsheets.

Remediation, as an iterative process, does improve with time. It is not unlike software programming where "regression testing" is often performed.

Robert Wucher
Principal
Wucher and Associates

One has to keep in mind, although the work is no longer performed in the IT department, the controls still do exist and are probably performed elsewhere. The most common example of this is in the payroll function. Payroll is an easy and cost-effective application to outsource. To ensure the proper controls are in place under this scenario, the auditors will rely on a report called the SAS-70.

The SAS-70 is essentially a report produced by independent auditors to document and sometimes assess the controls environment provided by the vendor. There are two types of these reports, a Type-I and Type-II SAS-70. Without going into too much detail on SAS-70 reports, the important difference to remember between the two is a Type I describes and documents the controls environment that is in place, while the Type II takes it a step further and independently tests the controls. In the back of a Type II report, there will be an auditor's assessment on the effectiveness of the controls and any discrepancies that have been documented. It is important for the system user to review and understand how these deficiencies may affect their reliance and use of the service provider's systems. Additionally, the report will also contain a list of "user control considerations." These are controls the service provider expects a user organization to review and implement in order to fully rely on the integrity of the externally hosted system.

Robert Wucher
Principal
Wucher and Associates

"The best way to ensure a control will pass an audit is to test it often and use large sample sizes."

- *Over 25 years of experience in the field of information technology (IT) at the senior and executive management level*
- *Areas of experience includes Sarbanes-Oxley (Section 404) IT Compliance and Auditing, Systems Auditing And Controls Review (SAS-94, SAS-70), Forensic Data Analysis and Auditing, Information Technology Strategic Planning, and Systems Selection And Request-For-Proposal (RFP) Development, among others*
- *B.S. in Business Administration from Old Dominion University*

Mr. Wucher can be e-mailed at robert.wucher@execblueprints.com

Systems may also be managed directly by the business process owner, such as a package-based accounting system being operated by an accounting department, a Web site being managed by a marketing or sales department, or simply an electronic spreadsheet being managed by a company's controller. Controls on these systems are as critical as any application managed by IT, as they may have a direct impact on financial reporting.

Another area to be considered is e-commerce. There are two types of these activities that are found in some businesses. These include (1) "Electronic Data Interchange" (EDI), where suppliers and manufacturer may electronically submit orders and invoices to one another, and (2) standard "Internet e-commerce activities," such as Web site sales or online donations. E-commerce activities may use such technologies as value added networks (VAN) or a third-party payment processor such as PayPal® or Verisign®. These types of systems may very well be within scope for SOX, and consequently, the controls that are in place to ensure their integrity must also be evaluated. This discussion leads directly into tip two:

Tip Two: Understand what is really required; not all IT controls are key controls and not all systems are in-scope for SOX.

One might suspect that there has been more than one company that has invested time into documenting and testing systems that have nothing to do with financial reporting. Common examples of these types of systems include the typically "online brochure"-type of Web site, which does nothing more than provide basic company information, such as an address and telephone number. Another example might include a contacts database used by the marketing or sales department.

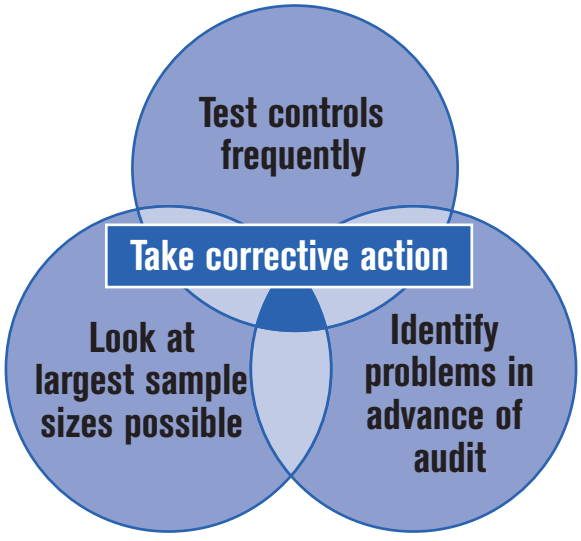
Not all controls are considered key controls. Many IT controls are simply complementary to a key control or serve as a secondary control. For example, a company may have controls in place to limit Internet surfing to what is called a demilitarized zone (DMZ) or it might use a virtual LAN (VLAN) configuration to limit access to key areas of the network from those who just need Internet access, such as a contractor. In this example, while limiting network access is always a good idea, this would not be considered a key control since the network security is likely governed by other components such as network level passwords and access security.

While there should be controls over every aspect of a company's IT infrastructure, including all types of systems, they probably have no direct impact on financial reporting and can be omitted from the process. One way to determine if a system is "in" or "out" of scope is to develop a comprehensive list of all applications. On the list, in a column next to the application name, it would be designated as to whether or not it is in scope and why. The list can be submitted to the auditors in advance of the audit to obtain concurrence. Once this activity has been completed, the focus of testing would be spent on the critical in-scope applications, which leads to tip number three:

Tip Three: Test, test, and retest the key controls.

The best way to ensure a control will pass an audit is to test it often and use large sample sizes. The auditors will evaluate and sample data from each quarter, so it is essential that company management also follows this approach. Some

Taking Control Before the Audit



While there should be controls over every aspect of a company's IT infrastructure, including all types of systems, they probably have no direct impact on financial reporting and can be omitted from the process. One way to determine if a system is "in" or "out" of scope is to develop a comprehensive list of all applications. On the list, in a column next to the application name, it would be designated as to whether or not it is in scope and why. The list can be submitted to the auditors in advance of the audit to obtain concurrence. Once this activity has been completed, the focus of testing would be spent on the critical in-scope applications.

Robert Wucher
Principal
Wucher and Associates

companies are fortunate enough to have a full-time compliance officer on staff to take the lead on this effort. Others use external contracting resources or automated compliance software. Still there are others that try to test the controls directly by themselves.

By testing controls frequently and looking at the largest sample sizes possible, management can identify problems well in advance of an audit and take corrective action. A common mistake is to simply wait a few months before the audit and then begin testing. Companies that follow this approach can quickly run out of time and may end up with unnecessary deficiencies cited during their audit. This leads directly into tip number four:

Tip Four: Allow plenty of time for remediation activities.

Remediation is never an easy process, and it does not matter how simple the effort may appear to be on the surface. The best place to begin is to develop a "living" remediation list. This is simply a list of the key IT controls that are in place at a company with the results of testing for those controls. The list should be actively reviewed and managed by a compliance officer, IT steering committee, and/or key managers.

An example of one common activity is to test a list of terminated employees against a list of active network user accounts. In many companies, there is almost always one employee that human resources may have neglected to notify IT to have that person's account deactivated. This is one example of a test that should be performed more often than on a quarterly basis, and it is an easy control to test and correct well before the audit begins. Fortunately, most IT controls are programmatic, where they involve a "machine setting" that does not change once it has been set, and probably will not require pulling a large sample to test.

Remediation, as an iterative process, does improve with time. It is not unlike software programming where "regression testing" is often performed. During this process, new software is tested over and over again until all of the bugs had been eliminated. This analogy is similar to IT SOX compliance remediation testing, which leads into the final tip, number five:

Tip Five: It really does get easier with each audit.

Many of the key controls have already been (or should have been) in place for some time; SOX only requires a company to fully document and test them. One of the most difficult aspects of becoming SOX compliant is to fully understand the key controls and their associated risks. Once this objective has been met, then testing becomes routine and results improve over time. IT activities that were once viewed as painfully arduous also become routine, and soon IT personnel forget there was ever a time when these activities were not already in place. Consequently, SOX implementation costs begin to decline, although one should keep in mind they never fully dissipate. ■

Ideas to Build Upon & Action Points

I. Breaking Down Sarbanes-Oxley Compliance

Sarbanes-Oxley is not just about compliance. Many companies are now requiring it of their vendors, and other companies are recognizing its benefits. Our authors point out that:

- Sarbanes-Oxley is about articulating objective standards for the integrity of information within the organization.
- Sarbanes-Oxley ensures that the same control processes are in place and functioning properly across the board.
- Sarbanes-Oxley compliance can yield positive results and cost savings.

II. The Bottom Line — Monitoring Impact

It is at the standards level that actual implementation occurs; this is also where results are visible.

When control systems are stabilized and in compliance, they will return results that create cost savings.

To monitor the impact of Sarbanes-Oxley:

- Look to standard organizations instead of just legal compliance experts.
- Look at SAS 70 Type II, but recognize its limits.
- Consider certification programs for individuals so that they can better understand the systems and where your company is in meeting compliance.

III. Must-Haves for Ensuring Successful Compliance

Create relationships.

- Compliance and IT should work together to identify areas for improvement and address those issues.
- Compliance is not a legal problem or a technology problem: it is a challenge requiring collaborative and creative strategies to build a framework and infrastructure.

Look at certification programs.

Enable your people to help the company in its goals.

Strike a balance between security, controls, and operational efficiencies.

- IT can police, but too much policing can result in a lack of cooperation.
- Strike a balance between IT's action and the right gadgetry to increase efficiency, automation, and data collection/analysis.

Test and retest.

- Test controls frequently, using the largest sample sizes possible.
- Identify problems well in advance of an audit.
- Take corrective action.

IV. The Golden Rules for IT's Involvement and Support

Employees and executives should think of Sarbanes-Oxley in terms of cost savings, not just as compliance. Sarbanes-Oxley is for the benefit of the company as a whole, not just investors or senior management. Therefore, IT should:

- Think about how automation and standardized data collection/reporting can reduce expenses across the company and increase efficiency, making people's jobs easier in the long run.
- Aim to create an auditable, enterprise-wide system for processing and reporting transactions.
- Look to gadgetry. If IT act solely as police, the result will be overkill. Instead, look to gadgetry and the options it makes available.

Likewise, IT must be encouraged through the early stages.

- Help IT to understand the key controls and their associate risks.
- Consider certification programs for IT individuals.
- Help IT through the first stages; testing will become routine, and results will improve over time.

V. Essential Take-Aways

An international company faces additional challenges.

- Different regulatory environments exist in different places.
- For example, the E.U. has specific data privacy and security constraints.
- U.S. companies must comply with foreign requirements or seek Safe Harbor provisions of the E.U. ■

10 Key Questions and Discussion Points

1. What are the top five tips every technology executive must know about Sarbanes-Oxley? How is the IT department affected by the list? Financially? Operationally? Does this represent a priority list? How focused should IT be on these top five topics?

2. What is the biggest misconception Chief Technology Officers and other technology managers have about the Sarbanes-Oxley rules? How can the CTO get accurate and insightful information about the law? What are the basic requirements? How can the CTO monitor changes and the impact of those changes?

3. What best practices push an IT department's compliance program over the top? Do the techniques require creative use of technology? In what way? What other departments contribute to the success of these practices? What role does leadership play? Who sets the tone?

4. What benchmarks are used to measure SOX compliance? How can a technology executive know if the firm is scoring well? What is measured and tracked? How? And by whom? What role does technology play in the measurement process?

5. How is ROI calculated for SOX compliance? What is measured? How? What is considered an acceptable ROI? What is the internal rate of return for technology investment directly related to SOX compliance?

6. What are the difficulties global firms face over domestic only companies? How are these challenges overcome? What additional costs are incurred by the global firm?

7. In your opinion, what percentage of a technology executive's time should be spent on SOX compliance? Has this increased or decreased in the last two years? To what do you attribute the change? Why?

8. What percentage of the IT budget is allocated to SOX compliance? What factors increase or decrease this allocation? What are the recurring costs? How can these be impacted by streamlining processes or technologies?

9. What are the creative methods companies have developed, in the last 12 months, in response to SOX? Are the development costs significant? What is the risk of adopting new technology that is not yet fully tested? What back up plans are required?

10. In the coming 12 months, how can IT departments work to reduce the cost of compliance? What new products are being introduced to help with reporting? Is training important to cost reduction? Who should be trained?