



Lessons Learned for SOX Compliance and Other Regulatory Challenges

Lessons Learned for SOX Compliance and Other Regulatory Challenges

Contents

Introduction	4
SOX transforms financial reporting—and IT controls	5
First-year reporting expensive and inefficient	6
SOX year two still a struggle to control costs	7
Major success factors for SOX compliance	7
Updated SOX guidance focuses on risk	10
GAIT principles may prove helpful	11
Emergence of data custody	12
Lessons learned from SOX compliance efforts in U.S.	16
Extending SOX lessons to data custody challenges	18
Appendix: IT Compliance Sources	19

Introduction

Initial experience with SOX costly, labor-intensive

According to most estimates, first-year efforts to comply with the Sarbanes Oxley Act of 2002, widely known as “SOX,” tended to overcompensate by trying to cover too many controls. Stacks of manual assessments and spreadsheets were produced at a very high cost. According to Ernst & Young, first-year SOX filers spent 70 percent of their time resolving deficiencies in IT controls in order to pass SOX audits.¹ In the second year of SOX activity, financial report filers still spent 60 to 65 percent of their time resolving IT deficiencies in order to pass SOX audits, and again experienced significant increases in personnel costs as they completed their final SOX audits.

Research reveals major success factors for SOX compliance

Recent research conducted among organizations in North America and around the world helps illuminate what appears to be working when it comes to SOX compliance. Organizations with the least IT control deficiencies:

1. Deliver continuous training to employees while ensuring accountability with policy
2. Restructure the risk management function, internal controls, and IT security
3. Reallocate IT expenditures by shifting spending from consultants and contract labor to automated tools
4. Automate IT measurements, reporting, controls, change management processes, and IT security policies
5. Focus on managing risk to improve IT controls, information collection, and reporting

Updated SOX guidance focuses on risk

A backlash of complaints from businesses implementing controls to meet SOX requirements led to new guidance updates by the Securities and Exchange Commission (SEC) in May 2005 and again in December 2006. This guidance has been offered to help management of public companies focus on analyzing the most significant risks, document logic for why these are the most significant risks, and choose the specific controls to assure integrity in financial reporting processes.

¹ *Emerging Trends in Internal Controls: Fourth Survey and Industry Insights*, September 2006: http://www.ey.com/global/content.nsf/US/AABS_-_Assurance_-_Internal_Controls_Summaries_Library

Lessons Learned for SOX Compliance and Other Regulatory Challenges

SOX eclipsed by data custody issues

While concern about the cost of SOX compliance will continue through 2007 and beyond, a new issue that can be termed “data custody” has emerged as a primary concern for organizations worldwide. Data custody is an “umbrella” phrase offered in this paper to represent the critical areas of data protection, data privacy, data retention, data destruction, and data discovery.

Recent research shows that within the past 12 months, the custody of sensitive data overtook SOX as the key regulatory challenge for many organizations. And, because nearly all sensitive data resides in information technology systems, the question of general IT controls and information security controls designed to safeguard sensitive data has come to the forefront.

Lessons learned

Despite the initial expectation that there was little connection between SOX compliance and information technology, IT controls continue to consume substantial resources among organizations that have successfully demonstrated SOX compliance through audit results. Organizations that achieved higher levels of SOX compliance (i.e., demonstrated fewer IT control deficiencies) have invested in the effort to successfully identify the IT controls needed to satisfy SOX (as well as comply with other regulations and internal policies) and then put procedures and tools in place to monitor, automate, and report on these controls.

The same behaviors that help establish SOX compliance and sustain results are also useful for dealing with the protection of sensitive data. However, the multitude of laws and regulatory issues surrounding the protection of data are not as concise or uniform as SOX, and can be far more complex, challenging, and potentially costly. Successfully dealing with data custody and privacy laws will require close attention to conflicting mandates, organizational policies, IT controls, monitoring of these controls, and reporting requirements.

SOX transforms financial reporting—and IT controls

On July 30, 2002, the Sarbanes-Oxley Act became law in the United States, changing forever the reporting landscape for finance professionals, executives of publicly traded companies, and ultimately, professionals managing and operating IT departments. Given the stiff penalties for fraudulent statements on the part of corporate officers required to certify the accuracy of financial reports (\$1 million and/or up to 10 years’ imprisonment for “knowing” violations and \$5 million and/or up to 20 years’ imprisonment for “willing” violations), top management understandably tasked its financial executives and auditors to do whatever was necessary to comply with the law.

Lessons Learned for SOX Compliance and Other Regulatory Challenges

Initially, the majority of early filers in the United States assumed there was little, if any, connection to IT departments or IT controls when first-year SOX audits were undertaken. The SOX law mandated several activities, including real-time disclosures, executive officer certification, increased transparency, audit independence, and SEC review of financial reports. It did not, however, specifically mention IT controls or the importance of IT's role in the compliance process.

First-year reporting expensive and inefficient

In a flurry of activity—and expense—publicly traded companies in the United States with annual revenues above \$75 million and their outside audit firms scrambled to meet the initial deadline. First-year (2004) compliance costs were substantial, according to Ernst & Young, with larger companies spending more than \$10 million to comply with Section 404 of the act.²

Much of the first-year expense in meeting SOX requirements was due to inefficient audits that involved confusion over how to define “material weaknesses in financial reporting,” inconsistent procedures, and duplication of effort by various departments. In many cases, companies relied on cumbersome manual methods for compliance, assembling a mix of spreadsheets, electronic messages, and audit tool reports. Rough sampling methods were used to verify the existence and scope of controls, with manual signoffs by individuals to certify accuracy.

Since many large corporations rely almost exclusively on computer systems to transact and manage financial information, IT departments soon became heavily involved. An Ernst & Young study of SOX implementation indicates that one in four companies with more than \$5 billion in revenue remediated more than 500 controls in the first year.³ The study showed that these first-year SOX filers spent 70 percent of their time resolving deficiencies in IT controls in order to pass SOX audits.

Perhaps not surprisingly, the E&Y study indicated that first-year SOX filers overspent on labor in their final quarter leading up to their final SOX audits as internal and external teams raced to meet the filing deadline. The E&Y study also showed that first-year efforts to comply with SOX focused significant time and effort on general IT controls, with more than 70 percent of the general IT control deficiencies associated with IT security. In many cases companies spent considerable resources simply determining which IT controls were critical to the audit process.

According to most estimates, first-year efforts at SOX compliance tended to overcompensate by trying to cover too many controls. Stacks of manual assessments and spreadsheets were produced at a very high cost. Amidst the flurry of first-year activity, however, many companies were forced to reexamine their existing systems of IT controls. In doing so, these companies realized they needed to try and narrow the scope of IT controls involved and find ways of automating those controls in their second-year reporting activities.

² *Emerging Trends in Internal Controls: Fourth Survey*, September 2005: http://www.ey.com/global/content.nsf/US/AABS_-_Assurance_-_Internal_Controls_Summaries_Library.

³ *Ibid.*

SOX year two still a struggle to control costs

In the second year of SOX compliance activity, financial report filers still spent 60 to 65 percent of their time resolving IT deficiencies in order to pass SOX audits, and again experienced significant increases in personnel costs as they finished their final SOX audits. The E&Y study reveals that 65 percent of the time and effort devoted to correcting deficiencies in order to pass SOX audits continued to be spent on general IT controls. However, with the help of IT professionals, companies are beginning to monitor and capture data so that they can automate the reporting process and make it more efficient and consistent.

Overall, general IT controls are evolving into more specific IT controls that are transitioning from manual sampling methods to automated rule sets that systemize controls according to specific policies. As a result, more companies are moving toward a kind of “continuous auditing process” that promises to make the IT controls aspect of SOX compliance more effective and, ultimately, less costly.

Major success factors for SOX compliance

Recent research conducted among organizations in North America and around the world may help illuminate what works when it comes to SOX compliance. To date, the IT Policy Compliance Group (see Appendix) has published a number of primary research reports on its Web site at www.itpolicycompliance.com. This research, between October 2005 and March 2007, indicates several attributes of organizations that consistently demonstrate compliance with SOX regulations.

Organizations that are most successful in complying with SOX mandates (those reporting the fewest IT control deficiencies) are consistently taking the following actions.

Deliver continuous employee training

Organizations that are most successful in meeting compliance mandates proactively implement training and accountability programs to support stated corporate policies. They ensure that all employees consistently participate in training and achieve certification for such training.

In contrast, the majority of organizations struggling to improve compliance with policies and reduce IT control deficiencies are also the least mature on almost all training and accountability capabilities and practices. The benchmark research shows organizations that establish a culture of enforcement and accountability from the top, recognizing that no one department can “fix the problem,” are much more likely to achieve and sustain compliance.

Restructure risk management and controls

Restructuring the risk management function requires executive management to designate an individual or group with the authority to bring together multiple departments and disciplines for the purpose of focusing on the most critical financial and business risks—and the controls needed to mitigate those risks. Once the essential controls have been identified, special emphasis needs to be placed on organizing these controls into a coherent system that bridges departmental silos and encompasses IT security controls.

Benchmark research from the IT Policy Compliance Group shows that of the top 10 causes of IT control deficiencies, business continuity is the only one that does not wholly involve IT *security* controls. Nearly 70 percent of identified IT control deficiencies are directly related to the quality of the controls that govern IT security. Thus, the current research suggests that improving regulatory compliance outcomes is directly related to improving measurements, controls, policies, procedures, and the management of IT security controls specifically.

Reallocate IT spending

For most organizations, effectively reducing costs and sustaining regulatory compliance means overcoming a significant number of deficient IT security controls. Defining, controlling, and governing these IT control deficiencies involves an improved mix of labor and automation in the IT department aimed at reducing costs and sustaining regulatory compliance results. In general, research benchmarks show that organizations spending more on IT security exhibit fewer IT control deficiencies. Moreover, those organizations are spending less on contractors and services, and more on equipment and software to implement automated, IT-based continuous controls monitoring. This in turn enables companies to be more effective when it comes to reducing IT control deficiencies and meeting compliance standards.

Automate controls, processes, and reporting

In the first two years of SOX compliance efforts, many organizations have recognized the necessity of identifying the most critical IT controls (and by extension, IT security controls) for the financial reporting process, reducing or consolidating the number of those controls, and then automating IT controls to make monitoring and reporting as efficient and consistent as possible.

Lessons Learned for SOX Compliance and Other Regulatory Challenges

Research indicates that nearly all IT security controls and procedures, for example, are now automated among the most successful organizations in compliance with SOX. Although most firms are improving IT security policies, standards, and documentation, those that report the fewest IT control deficiencies are singularly focused on documenting procedures, making changes to both business and technical procedures, and automating these processes as much as possible.

The top IT areas being automated by organizations with the fewest IT control deficiencies include IT change management and reporting, role-based access to IT resources, IT security technology controls, and monitoring and reporting (Figure 1). Further, the top three automation tools that industry-leading organizations are using to achieve compliance are those for:

- IT security change management, testing, tracking, and reporting
- Auditing, monitoring, and reporting
- IT policies, standards, controls, and documentation

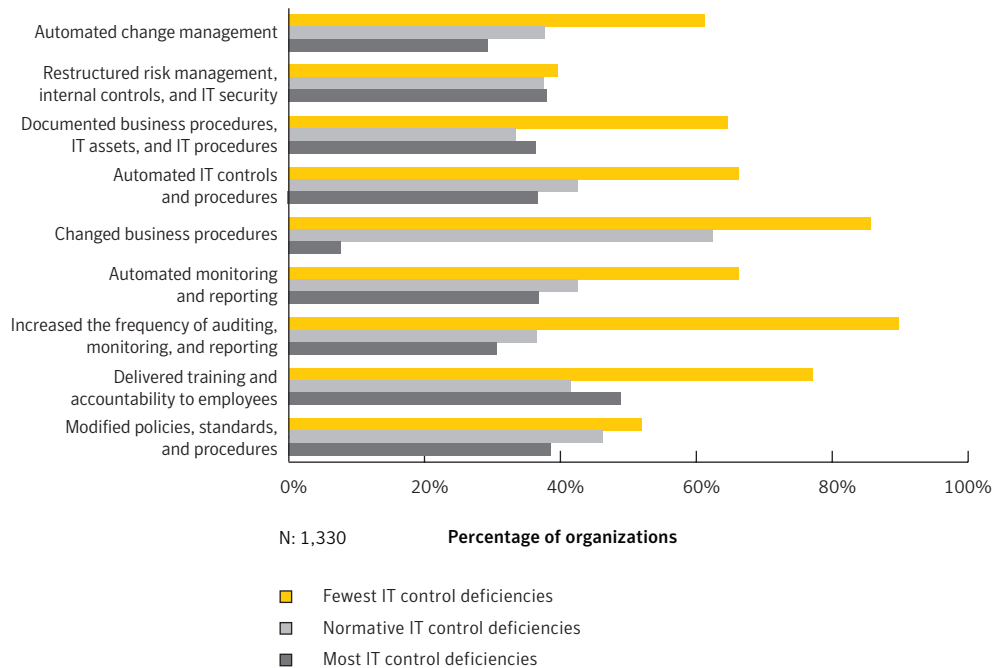


Figure 1. Actions taken to improve regulatory compliance results

Source: IT Policy Compliance Group, 2007

Focus on risk management practices and programs

Organizations with the fewest compliance deficiencies are implementing the most mature and continuous risk management practices and programs, covering all assets, most risk scenarios, and changes that are occurring, including those associated with the firms' customers, regulatory requirements, business, and IT operations. These "best practice" organizations have fully defined and implemented all of the technology controls and standards needed to enforce their own policies as well as those required by external regulatory mandates, law, and governing industry requirements.

Among organizations that have demonstrated the fewest IT control deficiencies, the most important capability stems from how data and knowledge are managed. Although data is not knowledge, the collection of data through IT controls so that the data can be transformed into actionable knowledge is a prerequisite. These firms are also collecting data, managing data, and reporting on a continuous basis; and they are conducting internal audits, monitoring IT security controls, and reporting at least monthly.

While a substantial amount of effort to achieve SOX compliance has involved IT controls, it is important to keep in mind that not all IT controls relevant to financial reporting reside within or under the authority of the IT department. In many situations, IT systems housed within various business units or subsidiaries that are functionally or geographically dispersed may not be accountable to a centralized IT department. Tax departments or credit departments, for example, may have developed their own applications or adaptations and may operate autonomously, entirely independent from centralized IT control or management. Organizations must assess their situations to determine where critical IT controls need to be located and adjust their compliance implementation plans accordingly.

Updated SOX guidance focuses on risk

A backlash of complaints from companies implementing SOX requirements led to new guidance updates by the SEC in May 2005 and again in December 2006. The goal of these updates was to help companies reduce excessive testing of controls and documentation, and reduce costs so that smaller firms (due to meet SOX requirements in 2008) can comply with the law without incurring excessive costs.

SOX Lessons in U.S. Can Apply to J-SOX

J-SOX is an unofficial name that refers to new Japanese legislation on financial reporting requirements similar to the Sarbanes-Oxley Act Sections 302 and 404 in the United States. According to Protiviti, a provider of business and technology risk consulting and internal audit services, J-SOX is part of a Financial Instruments and Exchange law passed in June 2006 that applies to more than 3,800 Japanese companies for fiscal years beginning on or after April 1, 2008. Thus, many companies in Japan are looking ahead to anticipate how to comply with the new legislation and are naturally curious to see if lessons learned in the process of meeting SOX requirements in the United States might apply to J-SOX.

At the end of 2006, Japanese officials released a draft of detailed "Evaluation and Auditing Standards" as well as "Implementation Standards" for J-SOX, which was finalized in early 2007. The evaluation framework is similar to United States SOX in that it includes an evaluation by management based on an internal control framework; it has an external audit requirement; and it focuses first on evaluating companywide internal controls, followed by process controls.

Unlike Section 404 of the U.S. law, under J-SOX the external auditor is not required to issue an opinion on the effectiveness of internal controls over financial reporting, but rather has to issue an opinion only on "management's evaluation of the effectiveness of internal controls." Thus, while the activities around documentation and testing of internal controls may be similar for J-SOX, their extent and scope is vague and undefined at this time.

Lessons Learned for SOX Compliance and Other Regulatory Challenges

Designed to clarify requirements related to SOX Section 404 (IT general controls), the new guidance directs auditors to leverage the work of internal corporate accountants, focus on controls associated with the greatest financial reporting risk, and consider company size when planning audit scope. The guidance suggests that management must focus first on what risks are most significant, and then define which controls to use in order to effectively monitor the processes associated with those risks.

The revised guidance will probably not rectify all of the objections of anti-SOX groups, and the updates do not exempt smaller companies from SOX accountability, as many small businesses had hoped. Moreover, financial audit firms would still be responsible for evaluating the business and IT controls for public companies, and these financial audit firms must interpret the guidance. Auditors have historically interpreted similar guidance very conservatively, and public companies will continue to be required to defend their choice of significant risks in the integrity of financial reporting, and the business and IT controls necessary to address those risks.

The language of the new guidance has already been criticized for its vagueness by organizations such as The Institute of Internal Auditors (IIA), the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute. Much like current rules, the new guidance is subject to wide-ranging interpretation and argument, and its impact on reducing the overall costs of SOX compliance is uncertain.

GAIT principles may prove helpful

Both the SEC and the Public Company Accounting Oversight Board (PCAOB) have recommended a “top-down, risk-based” approach to defining the scope and key controls of Section 404 of the SOX Act, focusing on the most likely or significant risks to financial reporting.

A set of four core principles has been developed by the IIA and presented in the Guide to the Assessment of IT General Controls Scope Based on Risk (commonly known as GAIT). The GAIT principles, along with a methodology, have been compiled specifically to help corporate managers and external auditors identify and implement the key controls that need to be monitored and reported out.

Principle 1: The identification of risks and related controls (such as change management, deployment, access security, operations) should be part of a top-down and risk-based approach used to identify significant accounts on a company’s general ledger, as well as the risks and the appropriate business and IT controls for processes and systems that underlie those significant accounts.

Many Japanese companies are understandably concerned about the potential costs of complying with the new legislation, and do not have a history of extensive internal auditing activities to fall back on. Because of language considerations, Japanese companies operating internationally have tended to decentralize their operations, including IT systems and operating practices, thus creating a major challenge in reporting across the entire organization. Practices such as the typical annual external audit connected with financial statements, commonplace among publicly held U.S. companies, are not as prevalent in Japan. Therefore, advisors to Japanese companies are encouraging them to begin the process of complying with the new law as early as possible. And, while minimum J-SOX standards—and penalties for violating those standards—may not yet be defined, management can begin preparing for J-SOX by determining which controls are most important, and where those controls apply in the financial reporting process.

Despite the differences between the U.S. and Japanese regulatory environments, the lessons for J-SOX appear to be fundamentally the same as those for implementing compliance with SOX in the United States. Obviously, Japanese companies have the benefit of more than two years of experience by larger U.S. organizations and will want to take advantage of the insights gained from that experience.

Lessons Learned for SOX Compliance and Other Regulatory Challenges

Principle 2: The risks that need to be identified are those that affect critical IT functionality in financially significant applications and related data.

Principle 3: The risks that need to be identified exist in processes and at various IT layers: application program code, databases, operations systems, and networks.

Principle 4: Risks in the IT general control process are mitigated by the achievement of IT control objectives, not individual controls per se.

Although these principles do not constitute a controls framework and do not include control objectives, they offer a tool that can help management and internal auditors determine relevant IT general controls on a consistent basis. The GAIT methodology enables organizations to implement the principles and gives management and auditors guidance around scoping IT general controls and the tools to defend these decisions. It provides an extended discussion on the principles, a detailed process for applying the principles, and a section with implementation examples.

In addition, the methodology helps organizations examine each financially significant application and determine whether failures in IT general control processes at each layer of the IT infrastructure represent a likely threat to the consistent operation of the application's critical functionality. If a failure is likely, GAIT identifies the IT general control process risks in detail and the related IT general control objectives that, when achieved, mitigate these risks. CobiT and other methodologies can then be used to identify the key controls that address these IT general control objectives.

The IIA provides more detailed information on GAIT principles and methodology through its Web site at www.theiia.org.

Emergence of data custody

While concern about the cost of SOX compliance as well as ongoing efforts to refine its interpretation will continue through 2007 and beyond, a new challenge that can be termed "data custody" has emerged as a primary concern for organizations worldwide. Data custody is an "umbrella" phrase intended to represent the critical issues of data protection, data privacy, data retention, data destruction, and data discovery. Because all of these data issues are related to one another in terms of management and handling and disposition of data, management will find it helpful to consider them together as "data custody."

Recent research shows that within the past year, the custody of sensitive data overtook SOX as the primary regulatory challenge for many organizations (Figure 2). And, because nearly all sensitive data resides in information technology systems, the question of general IT controls and IT security controls designed to safeguard sensitive data has come to the forefront.

While AMR Research estimates that SOX compliance has cost companies approximately \$1 billion per billion dollars of revenue, only one area of data custody—e-discovery—claims an even larger share of spending. Businesses now spend between \$2.5 and \$4 million per year on e-discovery

Lessons Learned for SOX Compliance and Other Regulatory Challenges

per billion dollars in sales, according to 2005 data from records management consultant Cohasset Associates. Companies that are involved in litigation and fail to preserve relevant electronic evidence, for example—or can't demonstrate that they have in place defensible e-discovery processes and policies—risk hefty fines, threats of criminal penalties, charges of obstruction of justice, and disruption of business operations.

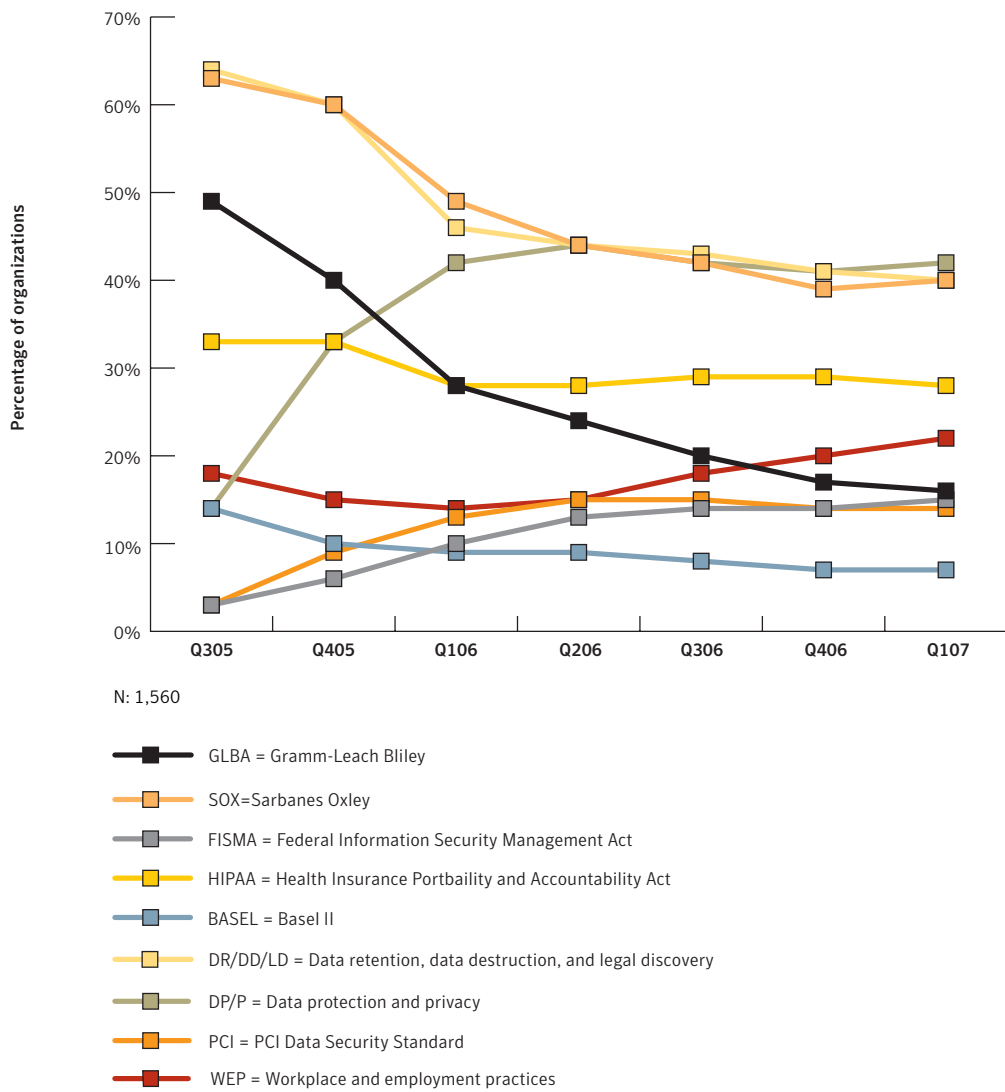


Figure 2. Changes in regulatory pressures
 Source: IT Policy Compliance Group, 2007

Lessons Learned for SOX Compliance and Other Regulatory Challenges

Data custody has become an organizational and IT priority primarily due to the changing regulatory environment and an explosion of laws across various jurisdictions governing data privacy and protection. Unlike SOX, which is one U.S. federal law interpreted and enforced by the SEC, data protection and privacy regulations have many sources—including more than 35 state laws governing privacy and data in the United States alone, as well as multiple regulations from the European Union. Add to this the fact that many companies operate in overlapping areas of the world, and the issue of data custody becomes a far more complex and confusing challenge than SOX or J-SOX—and potentially more costly and time-consuming.

On December 1, 2006, for example, several important amendments to the U.S. Federal Rules of Civil Procedure took effect. These amendments explicitly modified discovery procedures to address electronically stored information, or ESI. Falling under the issue of e-discovery, the changes impose express obligations on parties to preserve, disclose, and produce ESI. In one high-profile court case, Morgan Stanley & Co. had its legal position compromised as a result of poor or misrepresented e-discovery practices and policies that resulted in a \$1.6 billion verdict against the firm. Even though an appeals court has reversed the judgment against Morgan Stanley, the appellate decision was reached without resolving whether the trial court improperly entered a partial default against Morgan Stanley as a sanction for e-discovery misconduct. To learn more, visit www.ediscoverylaw.com.

Recent research has examined the issues surrounding data protection and its liabilities and suggested that actions to establish data custody IT controls are similar to those for SOX-related IT controls. For example, companies reporting the fewest data losses are taking six principal strategic actions to protect sensitive or classified data (Figure 3).

These actions include:

- Increasing the frequency of measuring and reporting on the efficacy of controls and procedures
- Delivering training to employees and contractors
- Modifying IT security controls and procedures
- Automating IT controls, procedures, monitoring, and reporting
- Segmenting/limiting access to sensitive data
- Holding employees accountable to policies and standards

Lessons Learned for SOX Compliance and Other Regulatory Challenges



Figure 3. Actions taken to improve data protection results

Source: IT Policy Compliance Group, 2007

The European Parliament has passed and is in the process of implementing a Data Protection Directive (95/46/EC), and independent data protection authorities now operate in 27 EU member states to oversee data protection, along with data protection initiatives established by governments around the world. For online links to government authorities that implement and monitor local and regional data protection and privacy regulations, visit the IT Policy Compliance Group Web site at www.itpolicycompliance.com/resources/government_regulator_links/wdpa.asp.

While the U.S. Congress may consider a national data protection law in 2007, it is unclear whether a federal bill will be able to satisfy privacy rights activists as well as business interests. A stalemate among legislators and interested lobbying groups may only prolong the uncertainty surrounding data custody and further add complexity to an issue that will likely grow more urgent in the future.

Lessons learned from SOX compliance efforts in U.S.

Despite the initial expectation that there was little connection between SOX compliance and information technology, IT controls continue to consume substantial resources among organizations that have successfully demonstrated SOX compliance through audit results. Organizations that achieved higher levels of SOX compliance (i.e., demonstrated fewer control deficiencies) have invested in the effort to successfully identify the IT controls needed to satisfy SOX (as well as compliance with other regulations and internal policies) and then put procedures and tools in place to monitor and report on these controls.

But, it is important to recognize that in the management of risk “one size does not fit all.” While executive management buy-in and organizational alignment to address SOX compliance challenges is critical, what constitutes successful application of IT controls to financial reporting will vary widely. Financial institutions, for example, may find that 10 to 20 percent of their IT controls involve significant risk in reporting financial results. On the other hand, a manufacturing firm may find that only a very small portion of IT controls has any significant impact on financial reporting systems.

Current primary and secondary research on compliance with SOX regulations does suggest several lessons learned from the experience of thousands of organizations in the United States. Those individuals or groups specifically charged with corporate regulatory compliance (i.e., Regulatory Compliance Officers) will need to consider all these lessons as they plan and supervise the implementation of compliance strategies for their own organizations.

Train employees: Senior management, in conjunction with human resources departments, needs to make sure that all employees receive continuous training in maintaining strict security and control measures within the financial reporting process while assigning specific individual accountability for controls.

Restructure risk management: Research suggests that organizations may have far too many controls that are not prioritized and may not directly affect the validity of financial reporting. Therefore, it is essential that management work with IT departments and internal auditors to restructure the risk management function and manage internal controls and IT security.

Lessons Learned for SOX Compliance and Other Regulatory Challenges

Reallocate IT spend: In most cases, companies can benefit by reallocating IT expenditures from spending on manual processes, whether performed by consultants or contract labor, to investing in IT tools that enable automation. The process of controls automation should help organizations to rationalize and shrink the total number of controls involved, and prioritize controls critical to managing the most significant risks.

Automate: To make the audit process more reliable and efficient and enable companies to adjust and sustain compliance over the long term, automation should focus on IT measurements, reporting, controls, change management processes, and enforcement of IT security policies.

Improve collection and reporting: Finally, organizations need to focus on managing IT risk to improve and unify IT controls information collection and reporting. Far too many companies are still struggling with “silos of execution” throughout their organizations.

Since these lessons have different impacts and affect the priorities of various departments and groups within organizations, the table below is provided as a quick reference guide.

Lessons learned by function

Lessons Learned	Senior Management	IT Management	Internal Audit	Corporate Legal
Continuous training and accountability for controls	X			X
Restructure risk management, controls, and IT security	X	X	X	
Reallocate IT spending		X		
Automate IT security monitoring, controls, reporting, and policies		X	X	X
Focus on managing risk to improve information collection and reporting	X	X	X	X

Extending SOX lessons to data custody challenges

Even though lessons learned from SOX compliance and managing IT controls in the United States can probably benefit those seeking to comply with J-SOX, these lessons can also be extended to the growing challenges of data custody. Particular behaviors associated with SOX—such as making risk management a priority, ensuring dollars are available to fund and manage IT controls, increasing the frequency of IT controls monitoring and reporting—should be similar for addressing data custody issues. The same identification, prioritization, and diligent use of IT controls can readily apply to data custody as well as to SOX compliance.

However, the multitude of laws and regulatory issues surrounding the protection of sensitive data are not as concise or uniform as SOX, and thus are far more complex, challenging, and potentially costly. Successfully dealing with data custody challenges and privacy laws will require close scrutiny of conflicting mandates, organizational policies, IT controls, monitoring of these controls, and reporting requirements.

Despite the extra effort and expense involved in meeting SOX requirements, the challenging process of passing audits over the past few years has forced publicly held organizations to examine and improve their IT controls and IT security. The current research suggests there is a strong correlation between how well companies manage IT controls and security, and their ability to achieve both policy and regulatory compliance—and how well they can expect to perform in meeting data custody requirements and related regulations.

Appendix: IT Compliance Sources

Ernst & Young

Ernst & Young, a global leader in professional services, is committed to restoring the public's trust in professional services firms and in the quality of financial reporting. Its 114,000 people in 140 countries provide a range of services centered on the core competencies of auditing, accounting, tax, and transactions. Further information about Ernst & Young and its approach to a variety of business issues can be found at www.ey.com/perspectives. Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited does not provide services to clients.

The Institute of Internal Auditors

Established in 1941, The Institute of Internal Auditors (IIA) is an international professional association of more than 122,000 members with global headquarters in Altamonte Springs, Florida, United States. Throughout the world, The IIA delivers certification, education, research, and technological guidance for internal audit professionals. More information can be found at www.theiia.org.

IT Policy Compliance Group

The IT Policy Compliance Group (IT-PCG) is dedicated to promoting the development of research and information that will help IT security professionals meet the policy and regulatory compliance goals of their organizations. The group supports a new Web site, www.itpolicycompliance.com, that focuses on helping organizations to improve compliance results by providing reports based on primary research as well as other related information and resources. Supporting members include The Institute of Internal Auditors, the Computer Security Institute, Protiviti, and Symantec.

Lessons Learned for SOX Compliance and Other Regulatory Challenges

Protiviti

Protiviti (www.protiviti.com) is a provider of independent risk consulting and internal audit services. The company offers consulting and advisory services to help clients identify, assess, measure, and manage financial, operational, and technology-related risks encountered in their industries. In addition, Protiviti assists in the implementation of the processes and controls to enable their continued monitoring. Protiviti also offers a range of internal audit services to assist management and directors with their internal audit functions, including full outsourcing, co-sourcing, technology and tool implementation, and quality assessment and readiness reviews. Protiviti, which has more than 50 locations in the Americas, Asia-Pacific, and Europe, is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world.

The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries.

More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2007 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. Printed in the U.S.A.
04/07 10579578