Analyst Perspectives™ Consensus Report

April 2008

Best Practices in SOX Compliance

Why Best Practices in SOX?

It is mandatory for public companies across the US to comply with the provisions of the SOX Act. Organizations may face financial penalties as well as reputational hassles in case of failure to comply, which can, in turn, lead to inefficient processes and controls within non-complying organizations. Experts believe that investors' confidence in organizations can be shaken owing to lack of accountability, reliability, and accuracy in corporate disclosures.

SOX experts believe that organizations fail these audits because a majority of the companies follow an event-driven approach for compliance. Moreover, the absence of documented control procedures can result in organizations failing SOX audits.

The issues of controlling processes, securing financial data, auditing, and managing documents' lifecycles, retention, and destruction have become top priorities for CIOs striving for SOX compliance. With most offices relying heavily on electronic documents and data, it is essential for companies to have a strategy for managing compliance as it relates to Section 404 of the Act (Source: "SOX Compliance Dos and Don'ts for CIOs", February 26, 2008, Andrew Gelina, Syrinx Consulting, Sarbanes-Oxley Compliance Journal).

SOX experts note that the companies face a burdensome task in complying with SOX regulations. Although SOX highlights the various requirements to be fulfilled by companies, it, however, does not provide any guidelines to achieve the set goals. Individual companies are left to their own devices, wherein they need to chalk out their own practices to comply with the mandate.

The Sarbanes Oxley Act was passed by the US Congress in 2002 to enforce financial accountability and control. It is aimed at protecting investors of US-based public organizations. The act helped in setting new standards for corporate governance, auditing, and financial reporting. Ensuring compliance with this particular act is a critical objective that faces public companies as well as those private limited companies planning to go public. According to the mandate of the act, public companies need to obtain a SOX compliance certificate each year. Therefore, organizations need to adhere to certain best practices/guidelines so as to meet the set objectives.

This report combines analyst perspectives, opinions, and expert recommendations about various best practices in SOX compliance.

Best Practices in SOX Compliance

Andrew Gelina, CEO of software development and consulting firm Syrinx Consulting, puts forth certain dos and don'ts for CIOs:

DOs

- **Start with good governance within the IT department:** Start with the IT department and look at what controls exist and which ones should exist. Implement governance in your own backyard first, pretending you are a separate "company within the company." Note the challenges you face, like system and process adoption, peoples' resistance to change, and technical hurdles. Dealing with these issues diplomatically and with deliberate strategy will help when you have to manage other areas of the company that do not report to you.

- **Tackle financials next:** Provide auditing and controls on financial systems. Get the CFO and his reports on board and let them know a SOX-compliant protocol for processes and procedures is coming in advance, and that it will not disrupt their ability to conduct business, but rather help to improve systems.

- **Build consensus:** To ensure system adoption and use, work across departments to collaboratively define the goals and rules of the compliance process, as well as the processes and procedures to be followed. If people do not have a say in the creation of the rules, they are less likely to follow them. Taking a "top-down, bottom-up" approach will help get people on board.

- **Fight fire with fire:** Leverage technology to help solve the compliance issue. By specifying security settings, storage policies, auditing policies, and expiration actions for business records in accordance with compliance regulations, you can help ensure your sensitive business information is controlled and managed effectively. Leveraging the right technologies can reduce the litigation risk for your organization.

- **Surface the data:** Make sure your solution provides dashboards for accounting and operational data. It should be easy to monitor ratios, keep an eye on actual versus forecast data, and flag any out-of-control metrics early. A well-developed dashboard that allows someone to easily see in red and green arrows how various metrics are holding up at the company makes things easier to manage.

"80 percent of the companies have 80 percent of the technology they need for SOX compliance" (Source: Sanjay Anand, Chairperson, SOX (GRC) Institute, [in Sarbanes-Oxley Guide for Finance and IT Professionals, 2nd Edition, published by John Wiley].

- **Show the proof:** Make sure your solution is auditable. If you cannot report on it, prove it, and guarantee your data integrity—in real-time or historically—your compliance effort effectively did not happen. Periodically pretend you are an auditor and look at your compliance initiative.

- **Keep it simple:** Define workflows that help enforce rules, but stick to what you need. Avoid over-engineering.

- **Re-use:** Leverage your existing authentication systems (Active Directory, Lightweight Directory Access Protocol [LDAP], etc.) for your compliance system. You are going to need to prove that only authenticated people accessed the system, so do not write another separate authentication system (and force people to manage another password).

- **Find someone who has done it before:** Engage experts to help with your project; that is, people with experience in SOX compliance and people with experience in the technologies you will use to comply.

- **Get organized:** SOX is not a one-time problem like Y2K. So it makes sense to organize your reporting, controls, and monitoring into a regular business-as-usual activity. Use a compliance calendar, and schedule your monitoring and reporting activities.

➤ DON'Ts

- **Drop a bomb:** Do not try to roll out a big, comprehensive solution to everyone at once. Plan to iterate; pick a small group of users and prototype the tools and processes. Learn from your first implementation, improve, and roll out to a wider audience.

- **Automate before analyzing:** Do not automate every current manual process without rethinking it first. Virtually any paper process can be replicated in digital form, but consider ways to streamline and install automated controls in the process as part of the exercise.

- **Forget about document images:** Do not forget about faxes, signed copies of documents, and digital signatures, which are all first-rate factors too. Consider embedding watermarking or version IDs in the headers/footers of documents to tie signed images back to electronic draft originals.

- **Shoehorn:** Do not force the fit. Find the right tool for the job—one that manages document versioning, retention, legal

"A company's IT division serves an integral role in the establishment, monitoring, and testing of internal controls. Without adequate software and technology, the processes related to internal controls would be lengthy and costly" (Source: Sanjay Anand, Essentials of Sarbanes-Oxley, published by John Wiley).

"As you gain more visibility into processes, you can actually streamline them [business processes], compress them, make them more efficient. Once you start to make business processes more efficient from a control standpoint, you eliminate errors and frauds. You're automatically making businesses run better" (Source: "Better processes drive falling SOX compliance costs", June 1, 2007, Sanjay Anand, Sarbanes-Oxley Institute).

holds, and compliance with auditing/reporting. Do not try to adapt a tool or a set of tools that are not meant for it.

- **Rely on disaster recovery:** Do not rely on your disaster recovery (DR) data backup strategy for compliance. Do not count on DR for archival purposes, or for "freezing" or "snapshotting" data for compliance efforts. Use a separate store for these. On the flip side, if you have a disaster and have to cut over to your backup site, you need to follow your compliance procedures there as well.

- **Rush to completion:** Do not sacrifice diligence and governance in the name of "getting it done." This applies to both implementing your initial compliance process as well as maintaining compliance while managing other projects at your company. It is better to figure out inefficiencies and areas of risk early and bite the budget bullet to ensure you have enough resources to complete the project in a realistic timeframe.

(Source: "SOX Compliance Dos and Don'ts for CIOs", February 26, 2008, Andrew Gelina, Syrinx Consulting, Sarbanes-Oxley Compliance Journal)

Info-Tech Research, an IT research and advisory company, sees strong interest among IT decision makers in the relationship between SOX compliance and the IT Infrastructure Library (ITIL) framework. There is, however, no straightforward connection between the two, even though certain applications of ITIL can help with SOX compliance, states Ross Armstrong, senior research analyst with the firm. Many enterprises will have run into the Control Objectives for Information and related Technology (COBIT) before considering ITIL. If SOX compliance is on the agenda, COBIT is not an option but rather a requirement. COBIT was published and is maintained by the Information Systems Audit and Control Foundation (ISACA) and the IT Governance Institute.

COBIT puts emphasis on the factors that matter most for risk management, security, consistency of data, and cost control. To this end, COBIT establishes 34 control objectives, each linked to a number of specific activities. These are tied together by means of a common control framework, supported by numerous management guidelines, as put forth by Armstrong:

- For SOX compliance only, go with COBIT. The SEC considers COBIT an acceptable control framework standard for governance, security, and internal control best practices. While COBIT adoption is not mandatory for SOX compliance, it is the de facto

framework to relate to SOX compliance. COBIT focuses on the following guidelines:

- Acquire and maintain application software.
- Acquire and maintain technology infrastructure.
- Develop and maintain policies and procedures.
- Install/accredit software technology infrastructure.
- Manage changes.
- Define and manage service levels.
- Manage third-party services.
- Ensure systems security.
- Manage the configuration.
- Manage problems and incidents.
- Manage data.
- Manage operations.

- IT shops with fewer than 10 employees should look at COBIT Quickstart, which is designed for small to medium enterprises. Info-Tech strongly advises the use of COBIT Quickstart to help small- and mid-sized enterprises (SMEs) meet compliance goals. COBIT Quickstart is a baseline for SMEs for whom IT is not mission-critical. Quickstart is a subset of the larger COBIT publication and contains only the most critical control objectives. These objectives were specifically chosen because they retain COBIT's fundamental principles, but can be implemented quickly.

- For compliance and service management, use COBIT and ITIL concurrently. ITIL maps well with COBIT, the de facto North American governance framework. COBIT is commonly used alongside ITIL to formalize the accountability links between various aspects of IT and the financial governance structure of an enterprise.

- For IT security-centric shops, adopt the ISO 27001 standard. ISO 27001 provides the framework and accreditation processes by which an enterprise designs, implements, manages, maintains, and enforces security processes and controls. Like other ISO cer-

SOX has demonstrated the value of IT to businesses. "IT has always been treated as separate from the business, which is really unfortunate. With SOX, IT has found a place where it is integral to the business. It is respected for that and regarded for that. IT is in the board room now" (Source: "Better processes drive falling SOX compliance costs", June 1, 2007, Sanjay Anand, Sarbanes-Oxley Institute).

tifications, ISO accreditation lets the world know that the enterprise is committed to high standards of quality, including information security.

- ISO 27001 compliance is completely optional for enterprises. Privately-owned enterprises can use the certification to demonstrate SOX levels of IT security when dealing with publicly-traded entities.

- Other benefits commonly associated with ISO certification include marketing potential to encourage new business opportunities as well as improved relations with existing business partners.

(Source: "SOX and ITIL: There Is No Dotted-Line Relationship!", February 22, 2008, Ross Armstrong, Info-Tech Research, Sarbanes-Oxley Compliance Journal).

Conclusion

- Organizations need to carefully assess their IT departments as a first step toward successful SOX compliance. Companies should check for the different challenges and hurdles that they might face in the process.
- The goals and objectives of the compliance process and also of the processes to be incorporated should be properly defined so as to ensure smooth system adoption.
- Leverage technology in resolving the compliance problem. To ensure that business information is handled effectively, companies should specify the security settings, auditing policies, storage policies, etc.
- Workflows need to be defined appropriately so that the rules are enforced and people stick to what needs to be done.
- Organizations should involve experts in their project, i.e., people who have substantial experience in SOX compliance as well as those who have the requisite technological knowledge for the compliance process.
- Firms need to consider methods/ways so as to streamline and replicate any paper process into digital form, as well as for the automation of manual processes.
- Companies should figure out the inefficiencies/risks involved with the compliance process in time, so that the budget is allocated accordingly and the project meets its realistic deadline.
- For technology related processes, organizations should try applying the COBIT framework.
- COBIT and ITIL should be implemented concurrently for compliance and security management.
- For IT security-centric shops, adopt the ISO 27001 standard. ISO 27001 provides the framework and accreditation processes by which an enterprise designs, implements, manages, maintains, and enforces security processes and controls.

References

"SOX Compliance Dos and Don'ts for CIOs", February 26, 2008, Andrew Gelina, Syrinx Consulting, Sarbanes-Oxley Compliance Journal

"Better processes drive falling SOX compliance costs", June 1, 2007, Sanjay Anand, Sarbanes-Oxley Institute, ComputerWeekly.com

"SOX and ITIL: There Is No Dotted-Line Relationship!", February 22, 2008, Ross Armstrong, Info-Tech Research, Sarbanes-Oxley Compliance Journal

SOX Guide for Finance and IT Professionals, 2nd edition, by Sanjay Anand, published by John Wiley

Sanjay Anand, Essentials of Sarbanes-Oxley, published by John Wiley

List of Contributing Firms

"Syrinx Consulting", Andrew Gelina

"Sarbanes-Oxley Institute", Sanjay Anand

"Info-tech Research", Ross Armstrong [mailto: rarmstrong@infotech.com]

AnalystPerspectives$^{SM/TM}$ is a subscription-based offering from Books24x7, a SkillSoft Company. For more information on subscribing, visit www.books24x7.com