by Thomas A. Cronin

Corporate Compliance: Pulling It All Together (Part 1)

Jan 22, 2004

Few people are speaking about tangible approaches for information technology (IT) to comply with such legislation as the Sarbanes-Oxley Act, Basel II requirements, and the USA Patriot Act. However, I will highlight a framework that includes practical approaches enabling organizations to build a compliance system once that can meet current and future government requirements. While I will focus on Sarbanes-Oxley (SOX) as an example of how to apply the framework, the framework is flexible enough that it can easily be adapted to meet other government requirements, such as those mentioned above. With regard to SOX, the framework identifies the key technology areas enterprises must leverage to meet the stipulations of the Act, and offers “best practice” advice for a smoother implementation.

SOX Framework

The Sarbanes-Oxley Act was passed in July 2002 to protect the investing public from officers of corporations and auditing firms who fraudulently misrepresent the financial stability of the corporation.

Sarbanes-Oxley Act mandates accuracy in financial statements and disclosures to a level unprecedented in recent history. Certifying corporate officers must know, not just believe that their company’s public financial statements are accurate and complete. The law also makes specific provisions for the retention of documents surrounding the audit process and public notifications due to material events.

There are a number of key provisions of the Act. One is good Control Point management, which is more than just a “best practice”-the Act requires it through law. As of December 2003, organizations should be completing activities related to identifying and documenting their key processes and the Control Points related to these processes. Once Control Points are defined, the next step is to implement Control Point surveillance to instantly identify (and notify certifying offices) about unusual behavior (“material events”). To achieve these objectives, we have created a SOX framework, which is designed to meet the requirements placed upon IT by the Act, but also is flexible enough that it can be adapted to other government requirements. The SOX framework encompasses existing tools, monitoring practices, system automation routines, and people to automate the surveillance of critical processes. Additionally, the framework bridges gaps in process monitoring. This is an essential element of achieving compliance.

Leverages IT

The SOX framework leverages IT in the areas of collaboration, reporting (real-time dashboards and reports), content collection and management, as well as core business/financial applications. Further, the SOX framework adheres to the principles of the Committee of Sponsoring Organizations (COSO), and it is designed to meet Cobit IT Control Objectives in support of IT compliance requirements.

Use of the SOX framework also helps overcome the problem that no one person or group has the necessary knowledge to implement all the required aspects of SOX Control Point surveillance and material breach notification. Pulling together the correct team to accomplish goals within a reasonable timeframe is important. The team must include individuals from diverse parts of the business to assure ready access to information for a quick, efficient, and effective SOX project. Obviously, the team must incorporate individuals with domain expertise in finance, business, legal, and technical disciplines.

Finally, the SOX framework also helps ensure that "best practices" are utilized for threshold screening, filtering, and time delay for executive notifications. Incorporating filtering safeguards prevents rushed problem notifications to higher-level managers. This can be especially important because it allows the right people to triage a potential event and help avoid erroneous notification to certifying officers, executive management, and internal/external auditors.

Explore related questions

- What is the COBIT framework and what does it do?
- How can identity security help my Sarbanes-Oxley Act (SOX) compliance?
- What expertise is needed for formalizing IT for Sarbanes-Oxley Act compliance?
- What are current global data protection and privacy regulations?
- How does IT and OT convergence impact cybersecurity compliance?

No Room for Ignorance

The Sarbanes-Oxley Act leaves no room for certifying officers to claim "ignorance" to the possibility of creatively engineered financial figures. It also removes any ability to state "lack of knowledge" in overlooking unethical practices. CIOs must now take on the challenges of: (1) enhancing their knowledge of internal control, (2) understanding their company's overall SOX compliance plan, (3) developing a compliance plan to specifically address IT control, and (4) integrating this plan into the overall SOX compliance plan.

More specifically, SOX requires the documentation of internal processes, the establishment of internal controls and disclosure controls, plus the monitoring and documenting of these controls. The Act also establishes the requirement that evidence must be provided as to the effectiveness of these controls.

Business process owners and the IT organization must translate new policies and procedures-concerning monitoring, testing, documentation and reporting generated by SOX compliance activities-into a working reality. It falls upon the shoulders of process owners and IT to detect events surrounding Control Points, evaluate these events, ensure events are recorded for evidence, and perform notifications within 48 hours (section 409 of the Act). It's easy to see that no one person or group has the necessary knowledge to implement all the required aspects of SOX Control Point surveillance and material breach notification. Pulling together the correct team to accomplish goals within a reasonable timeframe is important.

A Team Effort

SOX implementation is a team effort, and unlike Y2K, it is not going away at the stroke of midnight. The team that is assembled at this time will be the knowledge leaders for future modifications-which are inevitable.

Currently in the SOX compliance process, organizations should be concluding project activities related to Section 302 of the Act, which establishes the need for detailed documentation of critical processes, and the identification of Control Points related to these processes. It has been our experience that analyzing processes, and capturing and documenting the "Who, What, Why, and Where" are some of the most difficult tasks. Assembling the right people, communicating "Why" we are doing this, understanding "What" information is needed to monitor/capture, and "Where" the information resides are all critical success factors. Incorrectly performing these activities can lead to considerable expense to correct, and even result in jail time if done mischievously.

After establishing Control Points in accordance with Section 302, the follow-on steps are to establish monitoring (manual and/or automated) of the identified Control Points to comply with Sections 404 and incorporating the necessary testing and notifications to comply with Section 409. This is where the SOX framework comes in.

The SOX framework (highlighted below) was constructed to meet the requirements placed upon IT organizations by the Act. It was built to provide guidance for the many enterprises that are recognizing they do not have the surveillance infrastructure or workflow capabilities to adhere to Section 409 requirements. It also supports the requirement to

alert executives of material events within 48 hours of their occurrence, as well as to store and manage evidence for years.

SOX Framework

As illustrated, the framework identifies the key technology areas enterprises must leverage to meet the stipulations of SOX. The framework provides a clear picture and an integrated process for an organization's SOX compliance and reporting status.

The Base Systems depicted at the bottom of the illustration represent some of the key applications enterprises must monitor, and acquire data from, to assure Control Point validation and to detect fraudulent or suspicious activity. Surveillance also assures processes are operating and behaving as expected.

Next, Content Collection and Management applications work with, provide surveillance for, and manage the documented evidence related to Control Points. Business Activity Monitoring/Business Systems Management software automates surveillance. An external rules engine could also be used in concert with Operational Data Stores (ODS) or Content Management software. Content Management software administers the process of maintaining documented evidence, document tracking and storage.

At the Reporting level of the framework, we have re-performance testing and use of dashboards. Re-performance refers to computations made to independently verify the integrity of transactions or balances. Re-performance testing also relates to testing the operating effectiveness of key controls. Re-performance testing can be accomplished through Business Applications Management/Business Systems Management (BAM/BSM) software or can be handled though a combination of manual and synthetic transactions. Either way, the approach and results must be captured and maintained for the auditors. Dissemination of information is most easily accomplished through dashboards and reports tailored for each stakeholder group. Reports and dashboards can be built and distributed with BAM/BSM, Content Management, and/or Business Intelligence software.

At the very top of the framework, in the Collaboration Workroom, the project implementation team as well as virtual teams that may be assembled to investigate and resolve Control Point breaches can use collaboration software.

In my next article, I will clarify in more detail how the framework facilitates Control Point monitoring and management, as well as other key success factors to consider.