IT Auditors Turn to Cobit for Sarb-Ox Guidance
Thibodeau, Patrick
Computerworld; May 15, 2006; 40, 20; ABI/INFORM Complete
pg. 9

IT Auditors Turn to Cobit for Sarb-Ox Guidance

Companies use the IT governance guidelines to improve compliance

BY PATRICK THIBODEAU
ORLANDO

Increasingly, to keep themselves and their companies out of trouble, IT auditors are going by the book — the Cobit book on IT governance.

Cobit, formally known as the Control Objectives for Information and Related Technology, is a framework for governing IT and evaluating internal system controls. The guidelines have been around since the early 1990s, but the need to comply with the Sarbanes-Oxley Act is fostering new interest in them, according to attendees at a conference held here last week for IT auditors.

Sarbanes-Oxley "is an amorphous document — it says 'Have controls,' but it doesn't tell you what controls or how to have them," said Scott Thomas, an IT security manager at a large food services company that he asked not to be named.

Thomas said Cobit has given his company "a nice, solid process" to follow on Sarbanes-Oxley compliance, as well as a means for showing external auditors the security controls it has in place.

In Plain English

The framework also gives IT and business managers a common language on system controls, according to Thomas. Without Cobit, communication between the business and IT sides at his company often was "apples to oranges," he said at the conference, which was sponsored by the Information Systems Audit and Control Association (ISACA), based in Rolling Meadows, Ill.

Cobit explains in a "nontechnical way" how to build controls around a business process, said Steven Suther, director of information security management at American Express Technologies, the IT arm of American Express Co. in New York. The framework allows "my business folks to actually understand IT processes for the first time ever," Suther said at the conference.

ISACA offers free downloads of the Cobit framework and a related set of guidelines that are specific to Sarbanes-Oxley. Both were developed by the IT Governance Institute, which works in tandem with ISACA and is also based in Rolling Meadows.

A Version 4 update of Cobit was released in December, and a proposed second edition of the more focused IT Control Objectives for Sarbanes-Oxley document has been made publicly available for review and comment. The draft reflects recent controls-related guidance from the U.S. Securities and Exchange Commission and the Public Company Accounting Oversight Board. The comment period ends June 30.

Take Control

Here's a look at some of the recommendations found in the Cobit guidelines:

- Ensure that response-and-recovery activities are in line with prioritized business needs and that costs are kept at an acceptable level.
- Record information regarding all exceptions to internal controls and ensure that the underlying cause is analyzed and that corrective action is taken.
- Do formal training to ensure that all workers are aware of their compliance obligations. Responsibilities should be clearly explained.

SOURCE: IT GOVERNANCE INSTITUTE, ROLLING MEADOWS, ILL.

Complements ITIL

The controls management focus of Cobit differs from the data center orientation of the IT Infrastructure Library. But the two frameworks are complementary, and the latest version of Cobit includes improved integration with ITIL, said Robert Stroud, an IT service management evangelist at CA Inc. and a contributor to Cobit.

ITIL is focused on IT processes, such as how a help desk handles trouble tickets submitted by end users. Cobit takes issues to a higher level inside a company by focusing on meeting business needs, Stroud said. He noted that IT staffers who want to discuss, for instance, how much storage capacity is available aren't necessarily giving business managers the information they really need. "The business just cares about the ultimate service," Stroud said.

Meanwhile, the city of Phoenix is in the planning stages of a Cobit implementation, according to Lance Turcato, the deputy city auditor. Turcato, who previously was involved in a Cobit implementation within the private sector, said the framework can foster a better partnership among IT, business users and corporate auditors. ◗

Symantec Unveils Plan to Integrate Veritas Products

BY SHARON FISHER
SAN FRANCISCO

Symantec Corp. last week announced plans to pull together its various storage, server, application and database management technologies into an integrated offering.

At the annual Vision conference here for users of the former Veritas Software Corp., Symantec unveiled Data Center Foundation, which the company said will one day fully integrate the different tools it inherited when it acquired Veritas last July.

Officials from Cupertino, Calif.-based Symantec wouldn't comment on when the common integration platform will be completed. The company did say that "elements" of the technology have been deployed in some of its products and that integration features will be added gradually as new versions of its storage and server products are released in the coming months.

Over time, Symantec added, Data Center Foundation will provide users with consistent installation processes, user interfaces, workflows and license management policies.

"It's Utopia for me," said Brad Wood, senior director of enterprise technology at Corrections Corp. in Nashville, a private operator of prisons under government contracts.

Wood said the company already uses most of the storage products included in the Data Center Foundation blueprint. But, he said, "being able to see it under one business unit now, and the connections and its future — it's huge."

'Unifying Capability'

Data Center Foundation initially includes four main components, each consisting of several products. One is Server Foundation, a suite of server management tools that also was announced last week.

The individual products to be integrated include backup, media management, archiving, virtualization, server clustering, application management, provisioning and configuration management tools.

"If I can do less integration and work with our partners to deliver that unifying capability, I can focus more on cost takeout, efficiency of service, and service innovation itself," said Larry Lozon, vice president of data center services at Electronic Data Systems Corp.

Rick Villars, an analyst at IDC in Framingham, Mass., said the Data Center Foundation capabilities are similar to those available in storage virtualization devices such as TagmaStore from Hitachi Data Systems Corp. and InVista from EMC Corp.

"One of the big drivers behind storage virtualization was managing the proliferating number of servers connected to storage," Villars said.

Wood said he expects that the new system will be able to handle a variety of tasks, such as allocating new disks in response to high demand for data, and then report on them. Currently, Corrections Corp. has to manually add disks to arrays as needed, he said.

Villars said the Data Center Foundation plan is a good first step for Symantec. But in the long run, he said, "they need to connect the pillars into a more coherent system. That's the next step."

Over the long term, the various products in Data Center Foundation will be fully integrated using a configuration management database, said Robert Soderbery, vice president of product management for Symantec's data center management group. The different components "are silos right now," he acknowledged.

Soderberry said the integration plan offers many opportunities for Symantec, including an effort "to bridge the gap between the operational and the administrative world."

For example, he explained, if an operations manager saw an alert showing that a server was down, he could fix it himself rather than having to contact an expert to do it. ◗

NEW PRODUCT

Symantec Data Center Foundation

- Veritas NetBackup
- Veritas Storage Foundation
- Veritas Server Foundation
- Veritas i3 application performance management software