letters

csoletters@cxo.com

CSO

How to Reach Us

E-MAIL
csoletters@cxo.com

PHONE
508 872-0080

FAX
508 879-7784

ADDRESS
CSO Magazine
492 Old Connecticut Path, P.O. Box 9208
Framingham, MA 01701-9208

SUBSCRIBER SERVICES
Phone: 866 354-1125 Fax: 847 564-9453
E-mail: cso@omeda.com

REPRINTS
For article reprints (100 quantity or more), contact Jennifer Eclipse at PARS International at 212 221-9595 x237 or e-mail jeclipse@parsintl.com.

ABOUT IDG International Data Group (IDG), the leading global provider of IT media, research, conferences and events, informs more people about technology than any other company in the world. Offering the widest range of media options, IDG reaches more than 120 million technology buyers in 85 countries representing 95 percent of worldwide IT spending. IDG publishes more than 300 newspapers and magazines in 85 countries, led by the *Computerworld, Infoworld, Macworld, Network World, PC World* and *CIO* global product lines. IDG offers online users the largest network of technology-specific sites around the world through IDG.net (www.idg.net), a gateway to IDG's 330 websites powered by more than 2,000 journalists reporting from every continent in the world. IDG also produces 168 technology-related conferences and events, and research company IDC provides global market intelligence, analysis and forecasts in 43 countries.

SAS 70 and Other Kinds of Audits

THE ARTICLE ON SAS 70 ["SAS 70," November] states "service providers say they're being asked more and more often for SAS 70 audits, often instead of governance standards like Cobit or ISO 17799." Actually, Cobit [control objectives for information and related technology] and SAS 70 can work very well together.

Cobit is a globally accepted open standard framework that CSOs can use to directly focus on implementing and managing an organization's IT control and governance, which also dovetails with financial auditing standards such as SAS 70.

Cobit provides a comprehensive set of control objectives, including a subset for ensuring systems security. SAS 70 sets forth the process used by CPAs to audit the control objectives established by management. As a result, Cobit's framework is being used more frequently by CPAs when performing SAS 70 audits and for addressing international regulatory issues such as the Sarbanes-Oxley Act.

Most of Cobit is available as a free download from the nonprofit IT Governance Institute (*www.itgi.org*), made up of global business and IT leaders. Cobit 4.0, a significantly updated version with a stronger business-IT alignment focus, was released in December.

EVERETT C. JOHNSON JR., CPA
International President
IT Governance Institute
Rolling Meadows, Ill.

THE ARTICLE MISSES A POINT ABOUT SAS 70. First, a type 1 engagement refers only to the design of the controls. Their placement in operation and effectiveness is reserved for type 2 (a test of these controls is thus required under type 2). Secondly, SAS 70 reports are designed for opinions by CPAs that can then be used by other auditors. The typical example is a payroll service that a corporation relies on to record payroll expenses, but auditing the service company is not feasible. Instead, a SAS 70 report gives the corporation and its auditors comfort with respect to critical controls. Expanding on the use of SAS 70 for security audits is appropriate; however, making it the easy target for compliance is not appropriate because the assertions by management that are being examined by the CPA may not be sufficient under frameworks such as Cobit. I speak for myself, not my company.

YIGAL RECHTMAN, CPA, CISM
Person & Company, LLP CPAs
New York

BECAUSE OF THE UNIQUE NATURE OF a SAS 70 report, auditors have implemented an exhaustive list of policies, procedures and related controls that must be examined. Therefore, what makes this type of audit superior to any other type of internal control review is simply the scope of the engagement and the voluminous amount of information included in the final service auditor's report. While IT security consultants focus primarily on general and application controls, SAS 70 auditors emphasize these features and many more, such as operational issues, along with physical security guidelines and business continuity plans in the unlikely event of a disaster that interferes with your business. This is what makes SAS 70 superior to any other internal control review procedure.

CHARLES DENYER
Senior Manager, Tidwell DeWitt, LLC
Atlanta

More on Pharming

REGARDING "AFTER PHISHING? Pharming!" [October], you can secure your DNS infrastructure against DNS spoofing attacks effectively even without DNSSEC. A paper on securing Internet name servers is at *www.infoblox.com/library/whitepapers_external.cfm*. The presentation that inspired this paper is available via CERT at *www.cert.org/archive/pdf/dns.pdf*.

CRICKET LIU
Vice President, Architecture
Infoblox, Sunnyvale, Calif.

We want to hear from you.

To respond to articles you've read in CSO, write to us at **csoletters@cxo.com**. We welcome your criticism, thoughts and suggestions.