

THE TRUTH ABOUT SAS 70

CFOs who put too much trust in this high-profile report may be putting their companies at risk. BY DAVID McCANN

S

AS 70 CERTIFICATION VALIDATES THAT SABRIX operates as a certified and trusted outsourced tax research provider that meets the rigorous operational controls associated with Sarbanes-Oxley compliance.

That declaration, which resided at press time on the Website of Sabrix, a tax-management software-as-a-service (SaaS) provider, is typical of the language that SaaS vendors and other third-party service organizations use to highlight the importance of auditor reports that are based on the guidance known as Statement on Auditing Standards No. 70.

Yet the professionals that conduct SAS 70 audits and the organization that develops auditing standards both warn that such descriptions often mischaracterize the nature and purpose of SAS 70. While marketers routinely exaggerate the value of all kinds of external validations, from “Ten Best” car lists to “Best Places to Work” rankings, corporate IT decision-makers must beware this overreach, because as the rush toward SaaS and other forms of cloud computing accelerates, understanding the true capabilities of third-party service providers becomes more critical than ever.

A SAS 70 audit is a check on a service firm’s controls over processes and systems that could have an impact on the accuracy of entries in its customers’ general ledgers. Audit firms and the American Institute of Certified Public Accountants (AICPA) are concerned that as more service providers trumpet their receipt of a clean SAS 70 audit, misunderstandings about what the reports truly address will result in the finger of blame (and the lawsuits that may follow) being pointed at auditors for failures that lie outside the scope of SAS 70.

“The way SAS 70 reports are being marketed, service organizations are implying a level of assurance and trust that simply doesn’t exist,” says Dan Schroeder, a partner with accounting firm Habif, Arogeti & Wynne and chairman of the AICPA’s Information Technology Executive Committee. “It is grossly over the top.”

There are two types of SAS 70 audits. Type 1 merely describes the services provided and the financial controls in place with regard to them. Type 2, which is where the controversy mainly resides, additionally offers an opinion as to whether there was reasonable assurance that the controls were operating effectively during a defined time period. Any broader claims about what a SAS 70 audit means are likely to be invalid.

In part, that’s because SAS 70 reports are meant to be shared only with the service provider’s customers and the customers’ au-

ditors, for use in helping them evaluate controls over outsourced functions. Trying to claim that the mere existence of a report has value to *potential* customers, which is implicit in marketing activities, “doesn’t make sense,” says Chuck Landes, vice president of professional standards and services for the AICPA.

The implication that “because you have a report anyone can trust you to meet their specific needs,” says Schroeder, who specializes in SAS 70 audits, “is a misrepresentation of what SAS 70 is about.”

AUDITOR ANGST

What grates on the auditors, in particular, is the use of the terms “SAS 70 certified” or “SAS 70 compliant,” which they argue imply guarantees or the meeting of statutory or regulatory requirements that in fact don’t exist. A vendor voluntarily engages an auditor to prepare the report, and there is no specific criteria for its content. “When somebody says they are ‘SAS 70 certified,’ I have no idea what that means,” says Landes.

Sabrix says the language it uses in referencing its SAS 70 audit equates simply to a guarantee that it used a third-party independent auditor to examine its controls. “We’ve never misrepresented ourselves,” says Carla Yrjanson, vice president of tax research and content at Thomson Reuters, which acquired Sabrix last year.

There are many variations on the theme. Until July, NetSuite, one of the largest and most successful financial SaaS providers, said on its Website that its SAS 70 “certification” meant that it had “been through rigorous audit of its control over information technology and all related processes,” that customer data was “always backed up and safely stored,” and that it provided reliable service “now and in the future.”

Even if all those claims are true, Schroeder notes that they exaggerate what a SAS 70 audit actually addresses. Simply having a report doesn’t mean the audit was rigorous; no auditor uses words like *all* and *always* (which imply a guarantee); and auditors’ SAS 70 opinion letters explicitly note that they make no forward-looking representations.

When *CFO* inquired about the language NetSuite used, the company quickly changed the statement to say that the audit “documents that we have been through an in-depth audit of our control environment.” With the new language, according to Schroeder, “they got it right.”

SOC IT TO ME

Will new multitiered guidance restrain SAS 70 marketing hype?

FORGET ABOUT marketing overreach: service providers soon will have to stop talking about SAS 70 altogether. That's because it is set to be replaced next June with Statement on Standards for Attestation Engagements No. 16.

SSAE 16 will differ in some respects from SAS 70, but it will have the same narrow focus on controls over systems and processes that influence the accuracy of journal entries for service firms' customers.

The change is driven primarily by the ongoing effort to converge U.S. and international accounting and auditing standards, but the American Institute of Certified Public Accountants also frames it as part of a rebranding effort that it hopes will help clear up confusion over the scope of such reports.

The AICPA's Auditing Standards Board is creating a new umbrella, called Service Organization Controls, that defines three options for auditor reports on the controls of service providers:

Under **SOC 1**, which is synonymous with SSAE 16 (and is, in fact, available now), a service organization provides a very detailed description of its financial-related controls, to which the auditor will attest. Like SAS 70, SOC 1 is a restricted-use report, to be shared only with service providers' customers and their auditors.

SOC 2, a new option still being formalized, will be a similarly detailed examination of a service firm's controls over

security, privacy, confidentiality, availability, and processing integrity. The auditor will have discretion about whether to restrict the report's use, based on whether it is deemed relevant to the general public as opposed to just the service firm's existing customers.

SOC 3 represents a rebranding of the little-used Trust Services attestation, and will address the same five nonfinancial domains as SOC 2. But it is not based on detailed management assertions. Rather, the auditor opines on whether the service firm satisfies a set of more-general criteria for its control environment. It will continue to offer the option of a SysTrust seal, which is very much like a certification that can be used for marketing purposes, and the report itself can be made public.

"We think that once these additional alternatives are in place, it will help tremendously to clear up the marketplace," says Chuck Landes, the AICPA's vice president of professional standards and services.

But there will be nothing to stop vendors from making exaggerated marketing claims about their SOC 1 and SOC 2 reports, as they have for SAS 70. "The only way that situation will improve substantially is if businesspeople really understand what these new terms mean," says auditor and SAS 70 expert Dan Schroeder. "That will take a strong brand-messaging effort. There's a lot of work to do to turn things around." —D.M.

"We certainly want to be accurate," says David Downing, NetSuite's chief marketing officer. "If the use of the word *certified* was inaccurate [we wanted to correct it]." He also called on the AICPA to "get control of the process" and provide guidelines for vendors on how to communicate their SAS 70 status.

MARKETING MADNESS

Indeed, the auditing community may bear some of the responsibility for the misuse of SAS 70, suggests Jim Reavis, executive director of the Cloud Security Alliance. "There is a lot of misleading marketing out there," he says, "and the auditors are complicit to an extent. They understand the business model of cloud providers, but their own [business model] is to have a narrow scope. There's plenty of blame to go around."

Schroeder, in fact, says he frequently gets requests from service vendors to prepare SAS 70 reports for purposes that are outside their intended scope. Even firms with services that don't affect customer financial statements at all, such as HR or communications software, may try and sometimes succeed in getting SAS 70 audits done. Auditors who

take on such jobs may not be fulfilling their professional responsibilities, Schroeder says.

SAS 70 dates back to 1993, but it gained rock-star status after the 2002 Sarbanes-Oxley Act identified it as one way a firm could establish reasonable assurance that a service provider had effective controls over output to clients' general ledgers. That led most firms to include a SAS 70 audit on their checklist of requirements for such vendors.

Now, with the number of SaaS and cloud-computing providers mushrooming, there is a greater focus on what SAS 70 does and does not address. Vendor and auditor marketing departments aren't the only ones that should take that into account: so should customers.

"A SAS 70 should not be a replacement for good old-fashioned due diligence," says Joel Lanz, a CPA who provides technology-risk-management, IT-auditing, and data-security services to banks, and co-chairs the AICPA's Top Technology Initiatives task force. "A CFO should know that, but a lot of companies, especially smaller ones, don't do proper due diligence on vendors. They take the easy way out."

Proper due diligence, Lanz adds, goes beyond the assessment of financial con-

trols that is the province of SAS 70. The report may tangentially address system security and processing integrity, depending on the nature of the services and how the systems affect customers' financial statements. But, if done correctly, it does not cover controls that keep sensitive company information confidential or customer data private. Despite what vendors may say or imply, Lanz says, "privacy controls are not covered by SAS 70 audits."

Controls over aspects of data security, processing integrity, privacy, confidentiality, and system availability that do not affect the accuracy of service users' financial statements are more properly tested with an attestation called Trust Services. Relatively few U.S. service providers have embraced that option since it became available in 2003, says the AICPA's Landes. But the AICPA is hoping that some changes slated to take effect next year (see related story, above) will clear up some of the confusion over an auditing practice that is becoming ever more important. **CFO**

DAVID MCCANN (DAVIDMCCANN@CFO.COM) IS SENIOR EDITOR FOR TECHNOLOGY AT CFO.