



SAS 70s: Service Auditor's Report

How service organizations can demonstrate their commitment to internal controls



In an effort to show clients that airtight internal controls are in place, many companies are asking accountants to conduct a Statement on Auditing Standards No. 70 (SAS 70) review. The American Institute of Certified Public Accountants (AICPA) created the internationally recognized SAS 70 to show that an organization has been through an in-depth audit of its control activities, which generally include controls over information technology.

SAS 70 audits are required only of vendors who want to do business with publicly owned companies, but privately held companies also gain peace of mind by working with certified vendors.

Service organizations of all sizes can demonstrate their commitment to internal controls by proactively obtaining a Service Auditor's Report. In the past, SAS 70 audits were only performed for the largest service providers. But today, a Service Auditor's Report is crucial for service organizations of all sizes wanting to remain competitive in an increasingly crowded marketplace.

One of the key benefits of a SAS 70 report is it provides a single source of information in a standardized format that can be relied on when evaluating a service organization's controls.

Additionally, a SAS 70 report can also be used as a marketing tool, demonstrating to potential customers that your management has been proactive in obtaining the opinion of a reputable third-party as to the soundness of your organization's controls.

SAS 70s: Not just for the Fortune 500

When a company called Venture Encoding began printing checks in 1972, there wasn't much risk of losing customer data. As computers became commonplace, however, that risk increased.

Venture Encoding is now a \$30 million company based in Fort Worth, Texas, and today regularly handles confidential customer data as it processes auto and home loan statements, late payment notices, and e-payments, and manages online customer care tools.

"Ten years ago, if there was a breach in security or privacy, you could receive forgiveness and continue business as usual," says Kenny Hargis, Venture Encoding president and chief executive officer. "Today it just doesn't work that way. Our customers take privacy and security very seriously."



One reason for SAS 70 reviews rise in popularity is that companies need to be certain their outsourced service providers and contractors are as vigilant in protecting customer data as they are. Michael Gioja, chief information officer at Workstream, a workforce management solutions firm, started seeing SAS 70 requirements pop up in requests for proposals in the past couple of years.

“Clients want to be able to rely on you,” Gioja says. At Workstream, those clients include Chevron, Gap, Kaiser Permanente, Motorola, Nordstrom, Samsung and Sony of Canada.

Increasingly, laws require stricter protection of personal data. The Gramm-Leach-Bliley Act of 1999 demands financial institutions (and, by extension, their service providers, such as Venture Encoding) provide superior protection of client information.

While Gramm-Leach-Bliley is specific to financial institutions, Section 404 of the Sarbanes-Oxley Act of 2002 holds publicly held companies accountable for securing off-site data storage and confidential customer information. Payment Card Industry standards require that all companies involved with credit card transactions, follow a set of data security standards.

These laws and standards are resulting in more small-and mid-sized companies turning to SAS 70 audits as a way to prove that their financial and information security controls work.

“We’re being held to the same privacy and security requirements as the big banks and financial institutions,” Hargis says.



Venture Encoding recently received its SAS 70 Type II after a four-month examination. The SAS 70 Type II is more stringent than the Type I. Type I includes only a report on controls placed in operation at a specific time. In a Type II review, accountants actually test the controls to ensure those controls are operating effectively over the entire audit period.

At Venture Encoding, auditors tested the company for proper procedures in areas including control of access to customer data, encryption of customer data, change management, physical security of the building and intrusion testing. The final SAS 70 report would have noted if Venture Encoding had failed any of the tests. Auditors found no exceptions.



How to get started?

Before beginning a SAS 70 review, consider the following recommendations:

- Choose an auditor with appropriate expertise. Hargis of Venture Encoding was careful to choose an accounting firm with experience Conducting SAS 70 and other Information Technology (IT) risk management engagements.
- Define the right scope for the SAS 70 process. In completing a SAS 70 Type II audit, accountants review general and information systems controls that surround the processing of financial and customer data. These controls are specific and comprehensive. However, auditors might ask companies to include other controls, including information-security issues, such as access, user authentication and intrusion detection, in the audit as well. It's important that the audit include all the information security areas necessary to protect confidential information.
- First time for a SAS 70? Consider adding a preliminary review. Workstream, a publicly traded company with about \$32 million in annual sales, went through its first SAS 70 in 2006. Before embarking on the Type I and Type II audits, Gioja asked auditors to determine the scope of the services and controls that such reviews would cover, and to assess the general design of the controls so that Workstream could fix any gaps in the controls needed. This process is often called a SAS 70 Readiness Review.
- Talk to your clients before embarking on a SAS 70. The financial institutions that hire Venture Encoding conduct regular security audits of the firm. Venture Encoding leaders hope the SAS 70 audit will answer many of the questions raised by security audits conducted by each of the company's clients. "That's the intent," Hargis says. "We're pretty sure [the SAS 70] won't replace the need for those security audits. But it should increase our clients' comfort level with us." To make sure that happens, experts recommend talking to clients about specific control areas they'd like to see included in a SAS 70 audit. That is likely to save time on future security audits and reassure potential future clients.



Patience is a virtue.

Don't expect overnight results; SAS 70 reviews take time. At Workstream, auditors spent two months on the preliminary diagnostic review, three months on the Type I review and two months on the Type II review (after operating for six months following completion of the Type I review). Workstream is planning annual SAS 70 reviews, because current clients expect it, and future clients will require it. Venture Encoding will also be inviting auditors to return to Fort Worth annually to conduct SAS 70 reviews.

"In today's competitive landscape, you're going to have to have a SAS 70 to do



business with the big guys,” Hargis says.

How Freed Maxick & Battaglia can help with SAS 70 Service Auditor’s Report

Firmly grounded in the AICPA Statement on Auditing Standards (SAS) No. 70, our Service Auditor’s Report is one of the best ways for a service organization to differentiate itself from its competitors and clearly express a commitment to internal controls. We offer two types of SAS 70 reports:

- Type I – Reports on controls placed in operation
- Type II – Reports on controls placed in operation and tests of operating effectiveness

Throughout the SAS 70 engagements we keep our clients informed of our progress. At the conclusion of the project we present The Service Auditor’s Report, which contains a description of tests performed and our findings in the following areas:

- Operations and equipment
- Control environment
- Computer general controls
- Control over computer operations
- Control over access to programs and data
- Control over new development and changes to existing programs and systems
- Information systems
- User responsibilities

One of the key benefits of our report is it provides a single source of information in a standardized format that can be relied on when evaluating a service organization’s controls. A SAS 70 report can also be used as a marketing tool, demonstrating to potential customers that your management has been proactive in obtaining the opinion of a reputable third-party as to the soundness of your organization’s controls.

About Freed Maxick & Battaglia, CPAs and RSM McGladrey:

Freed Maxick & Battaglia is a locally owned firm, but also operates an alternative practice structure with RSM McGladrey, Inc., the sixth largest accounting and consulting firm in the U.S. and sixth largest internationally. With over 425 offices in 75 countries around the world, we have the resources to assist companies with global operations.

How do you benefit from our relationship with RSM McGladrey?

Through our formal arrangement with RSM McGladrey we have the resources of the 5th largest accounting firm in the United States, while still maintaining our independence and ability to make decisions locally. At a time when the Big 4 firms are exiting the Western New York market we have become the professional services firm of choice. We are the “alternative to the Big 4”. We’re different because we have the bench strength to provide a wide array of services with highly skilled professionals, but we are not burdened with the cost structure or bureaucracy of the national firms. These factors translate into world-class service at rates that are commensurate with the market you do business in.

For more information, contact:

Larry Hessney, CIA, CISA
Director, Enterprise Risk Management Services
Freed Maxick & Battaglia CPAs / RSM McGladrey, Inc.
tel: 585.271.2300
larry.hessney@freedmaxick.com