want independent validation and assurance? ask for a SAS-70

If your organization is preparing to enlist (or currently uses) a third-party service provider to initiate a process or record transactions on its behalf, you should request a SAS-70 audit report.

The term SAS-70 is a shorthand reference to two types of service audit reports described in Statement on Auditing Standards No. 70, Service Organizations, an auditing standard developed and issued by the American Institute of Certified Public Accountants (AICPA), originally for use by CPAs. In basic terms, a SAS-70 is produced as a result of an audit performed by a CPA to report on the processing of transactions by a service organization.

Traditionally, these reports were intended for use by CPAs only. But following the enactment of the Sarbanes-Oxley Act of 2002, their use shifted, and SAS-70s are now commonly shared between service providers and their clients.

Today, hospitals and health systems most frequently request SAS-70s from computer service providers. Often, computer service providers will present these reports to hospitals with which they desire to do business as an indication that their controls have been audited, usually in the area of information services. The focus is most often on information services simply because hospitals are most likely to purchase these types of services from these types of providers.

The practice of having CPAs audit computer service providers for potential hospital clients did not begin with SAS-70s. In the past, a computer service provider might, on its own volition, hire a CPA firm to review its operations and verify for a hospital client that it had adequate controls over its data processes. More recently, however, the requirements of Section 404 of the Sarbanes-Oxley Act led to interest in the broader use of SAS-70s for this purpose.

When Should You Request a SAS-70?
Hospitals tend not to use third-party service providers to process routine transactions. However, like companies subject to regulation by the Securities and Exchange Commission, hospitals today use third-party service providers for many other purposes—as pension record keepers, payroll providers, transfer agents, claims administrators, and custodial banks, for
example. Specific third-party service providers from which a hospital should request a SAS-70 include benefit administrators, market research firms, Internet service providers, group purchasing associations, investment advisers, application service providers, data centers, and investment fund administrators.

In short, determining whether to request a SAS-70 starts with a simple question: “Where are we sending data (either manual or electronic)?”

**SAS-70 Benefits**

Given all of the regulatory and compliance challenges that hospitals face, it is critical for them to be aware of the internal controls in place at their third-party service providers. With such awareness, a hospital can be sure the service provider meets the hospital’s needs and does not expose the hospital to needless risks. The primary benefit of a SAS-70 to a hospital is that it eliminates the need for the hospital to perform its own audit of each of its third-party service provider’s internal controls—a potentially cumbersome process, in which the hospital’s CPA might need to make numerous visits to and pursue multiple inquiries with each service provider.

With a SAS-70 from a third-party service provider, a hospital’s CFO has a reliable CPA’s validation of the third-party service provider’s internal controls, and the SAS-70 in many instances gives the financial leader more information than the hospital could obtain if it performed an audit itself.

Meanwhile, a SAS-70 allows the third-party service provider to have one audit and share the results with all of its hospital clients.

But what if the third-party service provider is unwilling to provide a SAS-70? If the provider’s services are potentially of great financial significance to the hospital, the hospital’s CFO should assess the situation to determine whether to proceed with the relationship. Under SOX, the lack of a SAS-70 could be a reportable significant deficiency in internal control. For this reason, the hospital should negotiate a SAS-70 as part of a contract with a third-party service provider. A work-around solution should not be an option.

**Report Types**

There are two types of SAS-70s, both of which consist of at least three sections: a CPA opinion, a description of controls, and information related to the design of the controls.

A type I report is issued for a specific date. Specifically, the CPA firm examines a third-party service provider’s controls on a given day, and reports on the processing of transactions and these controls for that day. This report is limited to an inquiry into and observation of the controls.

A type II report is issued for at least a six-month test period and is focused on the operating effectiveness of controls. Unlike a type I report, a type II report includes the results of the CPA firm’s testing of the controls over the test period. The SAS-70 describes the method that the third-party service provider uses to handle security, hardware, software, employees, data, procedures, and policies. There is no standard format for a type II report; the format and the control objectives can vary with each report.

On receiving a SAS-70, regardless of which type, the hospital’s CFO should thoroughly read the entire report, and not just peruse the summary, if one is provided. Having a full understanding of
the SAS-70 is important in the very least because the report may include details relating to the hospital’s responsibilities regarding the business relationship with the third-party service provider.

The SAS-70 Audit Process

When examining a third-party service provider’s internal controls for a type I report, the CPA might study the general and application controls within the provider’s computer system. Once this evaluation is completed, the CPA lists opportunities for improvement with proposed remediation and documents all audit-related information and activities.

If control remediation is necessary, the CPA can give the third-party service provider time to correct or strengthen the various internal controls. The CPA concludes the field work for the type I audit by conducting a final walk-through and examination of all internal controls, and then issues the report.

If the engagement progresses into the control design and testing phase, then the third-party service provider has requested a type II audit, which calls for at least a six-month design review and testing of the general and application controls within the computer system. In this instance, the CPA works with third-party service provider employees to review controls, test their effectiveness, and correct those that require remediation. Results are enumerated in the type II report.

The hospital recipient of either type of SAS-70 can expect to find within the report assessments of the third-party service provider’s elements of internal control. Depending on the SAS-70 scope, the hospital CFO might also find information on the system development life cycle (SDLC) approach, general computer controls, and application computer controls. Most important to the CFO is the section entitled “Client Control Considerations.” This section defines the controls for which the hospital organization is responsible. The client control considerations are complementary to the controls in the SAS-70 report for which the service provider is responsible.

Elements of Internal Control

Most SAS-70s provide information for understanding the service provider’s internal control structure in accordance with the COSO components. The report examines five internal control elements:

> **Control environment**—the foundation of the internal control system, as defined by fundamental discipline and structure
> **Risk assessment**—the service provider management’s ability to identify and analyze relevant risks in achieving predetermined objectives
> **Control activities**—the provider’s policies, procedures, and practices that ensure management objectives are achieved and risk mitigation strategies are implemented
> **Information and communication**—the means by which employees are informed of their responsibilities and provided sufficient time and resources to perform their duties, and—as such—the support for all other control components
> **Monitoring**—the external oversight of internal controls by management or other parties outside of a process, and the application of independent methodologies, such as customized procedures or standard checklists, by employees within a process

SDLC Approach

In the past, software development consisted of a programmer writing code to solve a problem or automate a procedure. Today, systems are so big and multifaceted that teams of programmers, analysts, testers, and users work together to create the programming code to make computer systems work. To manage this process, a computer service provider uses an SDLC approach to problem solving.

The controls under an SDLC approach deal with the sequence of events in the development of an information system (or application). The CPA looks to see whether the computer service provider’s SDLC process is ongoing, so that the cycle will repeat as a hospital undergoes changes in its business and information requirements. The CPA also seeks to verify that the SDLC process includes effective controls over system
design, authorization, programming, implementation (especially training), and acceptance by the hospital clients.

The SDLC approach should result in a high-quality system that meets or exceeds the hospital’s expectations. This systematic approach comprises several segments, each containing many steps and controls pertaining to the design cycle, development cycle, and testing cycle.

The CPA pays attention to the controls in each of these cycles. The SAS-70 should address concerns such as:

> Whether the service provider has controls (e.g., documentation) in place over operations to ensure the quality of the service features, such as effective, user-friendly screen layouts and the use of business rules, including the need to meet regulatory requirements
> Whether the service provider has controls in place to check for errors, bugs, and interoperability
> Whether the service provider has a quality assurance process

**General Computer Controls**

General computer controls apply to the system components, processes, and data that the computer service provider uses for the hospital. These controls ensure the proper development and implementation of applications, as well as the integrity of program, data files, and computer operations, and they therefore are extremely important in a SAS-70.

With respect to general computer controls, most SAS-70s cover five areas:
> Access controls
> Program change management controls
> Data center physical security controls
> System and data backup and recovery controls
> Computer operation controls SDLC controls, discussed separately previously, could also be regarded as falling into this category.

**Access controls.** These controls deal with the management of permissions for logging on a computer, and they therefore define the permissions that the hospital and other groups will require to access data. The CPA looks for a defined process for matching hospital user accounts to authorized users, detecting unauthorized access, and policing access by the computer service provider’s employees.

**Program change management controls.** These controls ensure that the computer service provider effectively monitors its computer system for changes to ensure that all changes are recorded, explained, documented, authorized, and successful. The CPA should seek to verify that the controls include testing and emergency change procedures.

**Data center physical security controls.** A considerable part of the SAS-70 process should be devoted to examining data center physical security controls. It is important for the computer service provider to show that policies are in place and are being followed effectively. To assess these controls, the CPA asks questions such as:
> How do people get access to the building? (For example, how are ID cards issued and security guards vetted?)
> Where is the computer equipment (hardware) kept and how is it secured from theft, fire, and flood?
> What are the policies dictating physical security?
> Who is alerted when intrusions are detected, and what is the policy for handling intrusions?

**System and data backup and recovery controls.** At the heart of these controls is the issue of disaster recovery. The CPA must verify that the computer service provider can restore information availability should all or part of the computer assets be destroyed or damaged. Risks to the data center include natural disasters, intentional and unintentional damage, theft, and hardware and software malfunction. Controls include a written disaster recovery plan; periodic back-up of the operating system, programs, and data; file-retention schedules; and a complete, written, and up-to-date computer asset inventory maintained off-site.
When assessing recovery controls, the CPA seeks to determine whether the computer service provider has sufficiently analyzed threats, explored all alternatives for an effective recovery plan, developed a plan with appropriate supporting documentation, and instituted appropriate periodic testing of the plan.

Computer operation controls. The CPA also must verify that the computer service provider has controls designed to ensure the ongoing, uninterrupted operation of the computer system; to provide reasonable assurance that the computer system is used for authorized purposes only; and to ensure that errors are detected and fixed promptly.

Application Controls
The purpose of application controls, which may be manual or programmed, is to ensure the totality and correctness of the hospital computer records. In a type II engagement, the CPA details in the SAS-70 the testing and operating effectiveness of these controls. In both types of SAS-70, the computer service provider may include information such as network diagrams or other supporting materials.

Client Control Considerations
The most important part of a SAS-70 to hospital CFOs is the section titled "Client Control Considerations." This section describes how the service provider and the hospital should work together to ensure effective controls. The hospital CFO also bears a responsibility to have rigorous internal controls and policies within the hospital to assist the service provider to do its job.

This section of the SAS-70 describes those control responsibilities that the service provider believes should be present at the hospital, particularly covering communication between the hospital and the service provider. The hospital's CFO should review the details of this section thoroughly and design and implement hospital-based controls to ensure the hospital fulfills all of its control responsibilities.

The importance of gaining a thorough understanding of this section should not be understated: Although reviewing the controls explained in the SAS-70 can seem tedious, the CFO needs to understand how the service provider is processing the hospital's data.

The CFO also should be aware of how much testing was performed by the CPA for the report, and understand the results. In a well-prepared type II report, the CPA testing includes large sample sizes. The CFO should review the SAS-70s with the hospital's CPA firm to ensure adequacy and reliability. The SAS-70 should encompass the full extent of the service provider's services that the hospital will use. For example, if the service provider is processing employee health benefit claims, the SAS-70 should state user controls.

Ask for a SAS—But Don't Get Sassy!
Traditionally, SAS-70s were intended for CPAs' eyes only. Now, as services providers have begun to make SAS-70s available to their prospective clients, hospitals have gained a valuable means to assess the quality of a potential business partner.

Nonetheless, hospital CFOs should not allow a SAS-70 to goad them into overconfidence: The report is not a guarantee, and it cannot reliably establish that the service provider is employing "best practice," meeting compliance requirements under the Health Insurance Portability and Accountability Act, or reducing the risk of fraud.

But it can give CFOs some peace of mind.

About the author
Christopher C. Boutin, FHFMA, CPA, CITP, is director, audit services, Baystate Health, Inc., Springfield, Mass., and a member of HFMA's Massachusetts-Rhode Island Chapter (chris.boutin@bhs.org).
Copyright of hfm (Healthcare Financial Management) is the property of Healthcare Financial Management Association and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.