



What is a SAS 70 Audit?

A SAS 70 audit is designed to provide information and assurance about controls within a service organization to user organizations (customers) and their auditors. A SAS 70 audit is conducted in accordance with the American Institute of Certified Public Accountants (AICPA) Statement on Auditing Standards (SAS) 70 standards. SAS 70 includes the professional standards used by a service auditor to report on the processing of transactions by a service organization for use by other auditors. A service organization is an entity (or segment of an entity) that provides services to a user organization that are part of the user organization's information system and control environment.

Who Uses a SAS 70 Report?

SAS 70 reports are primarily used by the service organization, its clients and the client's auditors. The client's auditors can use the SAS 70 to gain an understanding of the internal controls in operation at a service organization. Depending on the type of report, a client's auditors may be able to consider the service organization's internal controls in planning and executing their Sarbanes-Oxley 404 attestation and financial audit services for the user organization.

SAS 70 Report Sections

A SAS 70 Report typically includes several sections, including:

1. Independent service auditor's report
2. The service organization's description of controls
 - Overview
 - Relevant aspects of the COSO framework
 - Detailed description of controls
 - Control objectives, controls and user control considerations for each of the controls
3. Tests of the controls and results of the tests performed (for Type II reports)
4. Other information provided by the service organization

The Difference: Type I and Type II reports

A Type I report details the controls placed in operation as of a specific date. A Type II report details the controls placed in operation and tests of the operating effectiveness of controls during a specified period of time. The period of time for a Type II report is generally 6 months to 1 year. Since the Type II report is an extension of the Type I report, if you chose to do a Type I report and opted to switch to Type II, the difference is the application of tests of the operating effectiveness of specific controls. Some clients have opted for a Type I report for the first year and a Type II report in subsequent years. This has the advantage of allowing you to review and improve your controls before undergoing the testing in the Type II (with Sarbanes-Oxley 404 time pressures, this approach is less of an option).

SAS 70 Responsibilities

The service organization is responsible for:

- The service organization's description of controls
- Features of the entity-level controls that may affect the service provided to user organizations
- Applications and control objectives to be covered by the tests
- Other information the service organization may provide

In a type I report, the service auditor is responsible for:

- An opinion as to whether the service organization's description of its controls presents fairly those controls that have been placed in operation as of the end of the reporting period
- An opinion as to whether the described controls were suitably designed to achieve the specified control objectives
- Other information the service auditor may provide

In a type II report, the service auditor is responsible for:

- All items listed for a type I report
- An opinion as to whether the controls tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved for the period under review
- A description of the tests of operating effectiveness of controls and the results of those tests

Benefits of a SAS 70

- Satisfy customer financial audit requirements
- Satisfy customer Sarbanes-Oxley 404 requirements
- Compliance with regulatory requirements
- Satisfy contract requirements
- Documentation and testing of internal control structure

The SAS 70 Audit Process

A typical engagement would include:

1. On-site consultation to assist management in identifying the control objectives and control procedures
2. Provide guidance to management on the adequacy of their control objectives and controls
3. Perform on-site testing at various points in time to determine the effectiveness of the controls placed in operation and the operating effectiveness of the controls for Type II reports. Testing typically includes inquiry, inspection, and observation
4. Preparation of a draft report to be reviewed by the service organization for accuracy and completeness of the details
5. Delivery of a management letter to management for any control deficiencies uncovered during the course of the review
6. Issuance of the SAS 70 report in hardcopy and electronic PDF format.



SAS 70 Terminology

- **User Organization:** An entity that has engaged a service organization for a service.
- **User Auditor:** The auditor who reports on the financial statements of the user organization.
- **Service Organization:** An entity that provides services to a user organization.
- **Service Auditor:** The auditor who tests and reports on the controls of a service organization.
- **Service Auditor's Report:** A report issued by a service auditor over the internal control structure of a service organization.

Top SAS 70 Questions

What is Sarbanes-Oxley and how does it relate to SAS 70s?

In July 2002, the United States Congress passed the Sarbanes-Oxley Act ("the Act") into law. The Act calls for the formation of a Public Company Accounting Oversight Board (PCAOB) and specifies several requirements that include management's annual assertion that internal controls over financial reporting are effective (Section 404). In the case of Section 404, the independent auditor of the organization is required to opine on management's assertion over internal control in addition to the auditor's opinion on the fair presentation of the organization's financial statements. In order for management to make its annual assertion on the effectiveness of its internal controls, management will be required to document and evaluate all controls that are deemed significant to the financial reporting process.

Management will look to the service organization for information on the design and operating effectiveness of the service organization's controls if the organization uses the service provider to process transactions, host data, or other significant services. Management may obtain a SAS No. 70 service auditor's report from the service organization to gain an understanding of the service organization's controls and effectiveness of those controls.

Who can perform a SAS 70 audit?

A SAS 70 audit can only be performed by an independent certified public accountant (CPA) or firm. CPA firms that perform SAS 70 audits must adhere to specific professional standards established by the American Institute of Certified Public Accountants (AICPA). Member firms of the AICPA are required to follow specific guidance related to planning, execution, and supervision of the audit procedures. In addition, member firms are required to undergo a peer review to ensure that the firm's audits are conducted in accordance with generally accepted auditing standards.

Is there a list of SAS 70 standard control objectives and controls?

Since service organizations are responsible for describing their controls and defining their control objectives, there is no published list of SAS 70 standards. Generally, the control objectives are specific to the service organization and their customers. A service organization may consult with its service auditor for guidance on the control objectives.

Where can I get a copy of the SAS 70 audit standard?

The AICPA has released an audit guide entitled "Service Organizations, Applying SAS No. 70, as Amended." The audit guide is designed to provide the latest guidance to auditors of companies that use service organizations and service auditors that perform examinations of service organizations. The audit guide can be ordered from the AICPA's website and is listed as publication number 012772SK.

Does the entire organization have to be audited?

No, the SAS 70 audit should focus on the internal controls surrounding the services you provide to your customers. The service auditor's report can be customized to specifically identify the applicable data centers, operating environments and applications that are covered in the audit. An organization may have many business units while only one may process transactions or provide data processing services for its customers.

Can a SAS 70 audit be performed outside of the U.S.?

A SAS 70 audit can be performed outside of the United States. The audit engagement would have to be performed by a firm that subscribes to the AICPA professional standards.

How are SAS 70 audit reports generally distributed?

The result of a SAS 70 audit engagement is the issuance of a SAS 70 report. The SAS 70 report will then be provided to the service organization for distribution to their respective customers (user organizations), user auditors and other parties. The SAS 70 report is usually distributed via hardcopy or electronically.

For more information, please contact:

Mark Fulford, Risk Services Partner
(615) 309-2448
mfulford@lbmc.com

Paul Demastus, Risk Services Partner
(615) 309-2229
pdemastus@lbmc.com

