

## **SAS 70**

***Abstract- Statement of Accounting Standard No 70 (SAS 70), 'Reports on the Processing of Transactions by Service Organizations,' provides guidance to companies that outsource accounting tasks to service organizations.***

***The new standard is intended for all entities that use a service company for conducting transactions and maintaining related accountability and/or for recording transactions and information processing.***

***These entities would therefore include electronic data processing service centers, bank trust departments and mortgage banks. SAS 70 also provides guidelines to auditors engaged by service organizations to report on the internal control policies and procedures that have been adopted. Guidance is likewise given for testing the effectiveness of the internal control structure. SAS 70 replaces SAS 44, 'Special-Purpose Reports on Internal Accounting Control at Service Organizations.'***

The "expectation gap" SASs significantly changed auditing standards, but none more so than did SAS 55. It has led to an extensive rewrite of SAS 44 Special-Purpose Reports on Internal Accounting Control at Service Organizations. After three years' work, SAS 44 is being replaced by SAS 70 Reports on the Processing of Transactions by Service Organizations.

SAS 70 comes into play when one entity obtains one or both of the following services from another organization:

- *Executing transactions and maintaining related accountability; and*
- *Recording transactions and processing data.*

The organizations contemplated include not only EDP service centers but entities such as bank trust departments and mortgage bankers.

***The guidance may also be relevant where another organization develops, provides and maintains software used by the other entity.***

The SAS also has several specific exclusions such as banks processing normal demand deposit and checking transactions and joint ventures. SAS 70 gives guidance to the auditor of the organization using the service (user auditor) and the auditor of the organization providing the service (the service auditor).

## THE USER ORGANIZATION AUDITOR

The user auditor is required to obtain an understanding of the service organization's internal control structure to the extent necessary to be able to plan the audit and assess control risk. Where the service organization merely records and processes transactions and the user organization maintains accountability, it may be possible for the user auditor to ignore the service organization's internal control structure.

### PLANNING THE AUDIT

SAS 55 requires the auditor to gain an understanding of a client's internal control structure, i.e., its control environment, accounting system, and control policies and procedures, sufficient to plan the audit. The portion of the client's internal control structure that is resident at the service center is included in this requirement. In gaining the understanding of the service center's internal control structure, the auditor should consider factors such as:

- The significance of the financial statement assertions that are affected by policies and procedures at the service organization;
- The inherent risk associated with the assertions affected by policies and procedures at the service organization;
- The nature of the services provided by the service organization and whether they are highly standardized and used extensively by many user organizations or unique and used only by a few (frequently, user organizations have systems custom built by service organizations. If this is the case, it is more appropriate for the user auditor to perform the review than the service auditor.);
- The extent to which the user organization's internal control structure interacts with policies and procedures at the service organization;
- The user organization's internal control structure policies and procedures that are applied to transactions affected by the service organization's activities;
- The terms of the contract between the user organization--and the service organization for example, their respective responsibilities, extent of the service organization's discretion to initiate transactions, and other representations of the service organization;
- The service organization's capabilities, including its record of performance, insurance coverage, and financial stability;

- The user auditor's prior experience with the service organization;
- The extent of auditable data in the user organization's possession and
- The existence of specific regulatory requirements that may dictate application of audit procedures beyond those required to comply with GAAS.

The user auditor should also consider any available information in the user's possession about policies and procedures at the service organization, such as user manuals, system overviews, technical manuals, and third-party reports.

### **Assessing Control Risk Below the Maximum**

The user auditor may assess control risk below the maximum for particular assertions if one of the following exists:

- Results of tests of the user organization's controls over the activities of the service organization support such as assessment. (For example, the user auditor may test the user organization's independent re-performance of selected items processed by an EDP service center or test the user organization's reconciliation of output reports with source documents.);
- Consideration of the service organization auditor's report on policies and procedures placed in operation and tests of operating effectiveness, or a report on the application of agreed-upon procedures that describes relevant tests of controls supports such an assessment; and
- Results of appropriate tests of controls performed at the service organization by the user auditor support such as assessment.
- Regardless of the approach taken, the user auditor remains responsible for evaluating the evidence and for determining its effect on the assessment of control risk at the user organization.
- In addition, the user auditor should also keep in mind that the shorter the period covered by a test of effectiveness and the longer the time elapsed since the performance of the test, the less support for control risk reduction is provided.

## **THE SERVICE CENTER AUDITOR**

SAS 70 also gives guidance to auditors who are engaged to report on the internal control structure of service centers.

Because the work being done is not an audit of financial statements, the engagement is characterized as an examination in the SAS. The examination must be conducted according with GAAS, considering the nature and purpose of the engagement. This includes the requirements of SAS 53, The Auditor's Responsibility to Detect and Report Errors and Irregularities, and SAS 54, Illegal Acts by Clients.

### **SAS 70 provides guidance on two types of reports:**

Reports on policies and procedures placed in operation: A service auditor's report on a service organization's description of the policies and procedures that may be relevant to a user organization's internal control structure, whether such policies and procedures had been placed in operation as of a specific date, and on whether they are suitably designed to achieve specified control objectives.

Such reports may be useful in providing a user auditor with the understanding of the policies and procedures necessary to plan the audit and to design effective tests of controls and substantive tests at the user organization, but they are not intended to provide the user auditor with a basis for reducing his or her assessments of control risk below the maximum; and Reports on policies and procedures placed in operation and tests of operating effectiveness: In addition to the items enumerated in the report described above, the report states whether the internal control structure policies and procedures that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the related control objectives were achieved during the period specified. As with the first report, the second report may be useful in providing the user auditor with an understanding of the policies and procedures necessary to plan the audit. More importantly, it may also provide a basis for reducing the assessment of control risk at the user organization below the maximum.

### **Reports on Policies and Procedures Placed in Operation**

This type of a report expresses an opinion on the suitability of the design of control structure policies and procedures to accomplish specific control objectives specified by either the service organization or designated by outside parties such as regulatory authorities or user groups.

The description needed for the report is ordinarily obtained through discussions with service organization personnel and from service organization documentation--e.g., technical manuals and flow charts. The service auditor should determine whether the description provides sufficient information for user organizations and their auditors to obtain an understanding of those aspects of the service organization's policies and procedures that may be relevant to the user organization's internal control structure. In addition, the service auditor must establish that the relevant policies and procedures have been placed in operation. The service auditor need not test their operating effectiveness unless the second type of report is desired.

Although the reports on policies and procedures placed in operation is as of a specified date, the service auditor should inquire about changes to policies and procedures that occurred prior to the commencement of field work. The service auditor's report should describe any significant changes which are not included in the service organization's description. Changes which occurred more than one year prior to the date of the report are not considered significant. A service auditor's report on a description of policies and procedures placed in operation at a service organization should contain:

- Specific reference to the applications, services, products, or aspects of the service organization covered;
- Description of the scope and nature of the service auditor's procedures, and identification of the party who specifies the control objectives;
- Indication that the purpose of the service auditor's engagement was to determine whether 1) the service organization's description presents fairly, in all material respects, those aspects of the service organization's policies and procedures that may be relevant to a user organization's internal control structure, 2) those policies and procedures had been placed in operation as of a specific date, and 3) those policies and procedures were suitably designed to meet specified control objectives.
- Disclaimer of opinion on the operating effectiveness of the policies and procedures;
- The service auditor's opinion on whether the description presents fairly, in all material respects, the relevant aspects of the service organization's policies and procedures as of a specific date and whether, in the service auditor's opinion, the policies and procedures were suitably designed to provide reasonable assurance that the control objectives specified by the service organization would be achieved if those policies and procedures were complied with satisfactorily;

- Statement of the inherent limitations of the potential effectiveness of policies and procedures at the service organization and of the risk of projecting any evaluation of the description to future periods; and
- Identification of the parties for whom the report is intended.

If the service auditor believes the description is inaccurate or insufficiently complete for user organizations and their auditors, his or her report should so state, giving sufficient detail to provide with an appropriate understanding. The service auditor should report if there are significant deficiencies in the design or operation of the policies and procedures.

When complementary user organization procedures are necessary for the proper functioning of the controls, the procedures should be included in the description of the relevant policies and procedures. The service auditor's report should clearly indicate this requirement.

Reports on Policies and Procedures Placed in Operation and Tests of Operating Effectiveness. In addition to performing all the procedures previously described, the service auditor will apply tests of controls to determine whether specified policies and procedures are operating with sufficient effectiveness to achieve specified control objectives.

The report includes all the elements described for the first type of report. Because it makes a statement about the effectiveness of the controls, the report also contains the following:

- A reference to a description of tests of specified service organization policies and procedures designed to obtain evidence about their effectiveness in meeting specified control objectives. The description should include the policies and procedures that were tested, the control objectives the policies and procedures were intended to achieve, the tests applied, and the results of the tests. The description should include an indication of the nature, timing, and extent of the tests, as well as sufficient detail to enable user auditors to determine the effect of such tests on user auditors' assessments of control risk. To the extent that the service auditor is able to identify causative factors for exceptions, to determine the status of corrective actions, or to provide other relevant qualitative information about exceptions noted, such information should be provided.
- A statement of the period covered by the service auditor's report on operating effectiveness of specified control policies and procedures.

- The service auditor's opinion on whether the internal control structure policies and procedures that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the related control objectives were achieved during the period specified.
- A statement that the service auditor does not express an opinion on control objectives not listed in the description of tests performed at the service organization when all the control objectives listed in the description of policies and procedures placed in operation are not covered by tests of operating effectiveness.
- A statement that the relative effectiveness and significance of specific service organization policies and procedures and their effect on assessments of control risk at user organizations are dependent on their interaction with the policies, procedures, and other factors present at individual user organizations.
- A statement that the service auditor has performed no procedures to evaluate the effectiveness of policies and procedures at individual user organizations.
- A statement of the inherent limitations of the potential effectiveness of policies and procedures at the service organization and of the risk of projecting to the future any evaluation of the description or any conclusions about the effectiveness of policies and procedures in achieving control objectives.

The SAS provides for the service organization to specify whether all or selected applications and control objectives will be covered by the tests of operating effectiveness. In addition it provides for the designation of specific control objectives by outside parties such as regulatory authorities or a user group. In the absence of control objectives established by such outside parties, the service auditor should be satisfied that the control objectives, as set forth by the service organization, are reasonable in the circumstances and consistent with the service organization's contractual obligation.

The SAS requires that tests of controls should be applied to the control policies and procedures in effect throughout the period covered by the report, ordinarily a minimum of six months.

The report should refer only to the suitability of the design of control structure policies and procedures intended to accomplish specified control objectives and not to the suitability of the design of applications or processes to meet objectives beyond the specifically identified control objectives.

## WRITTEN REPRESENTATIONS OF MANAGEMENT

The service auditor should obtain a written representation letter from the service organization's management that:

- Acknowledges its responsibility for establishing and maintaining appropriate control structure policies and procedures relating to the processing of transactions for user organizations;
- Acknowledges the appropriateness of the specified control objectives;
- States that the description of internal control structure policies and procedures presents fairly, in all material respects, those aspects of the organization's policies and procedures that may be relevant to a user organization's internal control structure;
- States that the internal control structure policies and procedures, as described, had been placed in operation as of specified date;
- States that management believes its internal control structure policies and procedures are suitably designed to achieve specified control objectives;
- States that management has disclosed to the service auditor any significant changes in policies and procedures that have occurred since the service organization's last examination;
- States that management has disclosed to the service auditor any illegal acts or irregularities committed by service organization management or employees who have significant roles relevant to the processing performed for user organizations; and
- States that management has disclosed to the service auditor all design deficiencies in internal control structure policies and procedures of which they are aware, including those for which management believes the cost of corrective action may exceed the benefits.

Where tests of operating effectiveness were performed, the representation should state that management has disclosed to the service auditor all instances of which it is aware, of policies and procedures not operating with sufficient effectiveness to achieve related control objectives.

## HOW LONG A PERIOD TO TEST

To eliminate the relatively short time periods used by service auditors under SAS 44 (sometimes as short as one day), SAS 70 adopted the flexible approach of SAS 55--i.e., the longer the period covered by the test, the greater the support for control risk reduction. However, it then mandates a six month minimum. This six month requirement may not always be cost justifiable. For example, when testing access controls, the testing of such controls may require repeated visits to the service center.

## DEFINITIONS

*User organization* -- The entity that has engaged a service organization and whose financial statements are being audited

*User auditor* -- The auditor who reports on the financial statements of the user organization

*Service organization* -- The entity that provides services to the user organization

*Service auditor* -- The auditor who reports on the processing of transactions by a service organization and reports on policies and procedures placed in operation -  
- A service auditor's report on a service organization's internal control structure, on whether such policies and procedures had been placed in operation as of a specific date, on whether they are suitably designed to achieve specified control objectives, and on whether the internal control structure policies and procedures that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the related control objectives were achieved during the period specified.