



Shared Assessments Program AUP and SAS 70 Frequently Asked Questions

Q How is a Shared Assessments Agreed Upon Procedures (AUP) report different from a SAS 70 Type II examination report?

A The Statement on Auditing Standard #70 (SAS 70) and Shared Assessments Agreed Upon Procedures (AUP) are two different reporting standards promulgated by the American Institute of Certified Public Accountants (AICPA).

The SAS 70 was created as an “auditor-to-auditor” communication to help financial statement auditors understand the internal controls in place at service organizations used by their clients. The SAS 70 report is designed to facilitate communication about pertinent elements of a service organization’s controls. The report consists of an auditor’s opinion(s), the service organization management’s description of the controls (typically organized by the five elements of the COSO framework), the tests of design and operating effectiveness of the controls performed by the service auditor, and the results of those tests.

There are two types of SAS 70s: Type I, which excludes tests of operating effectiveness; and Type II, which includes tests of operating effectiveness. (These FAQs refer to the SAS 70 Type II report, which is the most common.) SAS 70s cover a set period of time, generally six months to one year.

In Shared Assessments Agreed Upon Procedures (AUP) engagements, two or more parties engage a third party to perform certain specified procedures, to which all the parties have agreed. The auditor performs the procedures and reports back to the parties on the results of those procedures. The procedures may take many forms and cover a wide variety of subjects. However, the two parties must agree that the procedures are sufficient for their particular purposes. The AUP report is presented in a simple format, with the procedures performed and their results. The AUP report contains no conclusions or opinions on the part of the auditor, only statements of fact. Financial institution regulators have suggested that it is important for financial institutions to evaluate AUP results in the context of their own internal risk control environments. Thus, it is the report *recipient* that evaluates the AUP test results, not the assessment firm.

Q How is the scope of a SAS 70 report different from that of a Shared Assessments AUP report?

A Traditional SAS 70 reports were not designed to meet the needs of financial institutions in certain areas, particularly information security. Thus, the scope of a Shared Assessments AUP is more detailed in those areas.

A SAS 70 examination addresses control objectives established by the service provider. The control objectives may include any number of processes performed by the service provider that are part of the financial information system of that organization’s client. The service provider’s auditor has a responsibility to make sure the control objectives address all aspects of the processing that may be relevant to the client’s auditors.

The scope of procedures performed in an AUP engagement is determined by the parties that need the procedures performed. The third-party practitioner is only responsible for executing the procedures and reporting the results. The Shared Assessments AUPs were developed by information security professionals from member financial institutions, service provider organizations, and certain assessment firms, and are reviewed regularly to ensure that the Shared Assessments Program is responsive to current threats in the financial services industry.

Q How do the procedures performed in a SAS 70 report differ from those performed in a Shared Assessments AUP report?

A While tests of operating effectiveness are performed in a SAS 70, an AUP engagement by definition is simply the performance of “agreed upon” procedures.

In a SAS 70, the procedures performed allow the auditor to form an opinion as to whether the control objectives have been met. Auditors determine which controls should be tested and what test procedures are necessary.

The Shared Assessments AUP is a standard set of procedures developed to address specific industry needs. An AUP report is based on the procedures performed and their results.

SAS 70s may also cover automated and manual process controls, as well as all relevant areas of IT general controls. Today’s Shared Assessments AUP reports primarily cover access controls and a limited number of business continuity controls, though the scope may be expanded over time.

To further make the distinction, consider a typical logical access control objective that might be included in a SAS 70 report: “Controls provide reasonable assurance logical access to data and programs is restricted to authorized individuals.” The service provider would provide its service auditor with a description of the controls that it believes would accomplish this objective. The auditor would review the service provider’s description of controls and independently select control activities for testing that he or she believes will provide “reasonable assurance” that the control objective was met during the period covered by the report.

With the Shared Assessments AUP, the procedures to be performed are defined by Shared Assessments Program members, reflecting their best judgment about which tests would best inform interested parties about a service provider’s ability to achieve targeted security performance thresholds.

Q Who may receive a Shared Assessments Program AUP report vs. a SAS 70 report?

A AICPA standards limit the distribution of both the SAS 70 and the AUP. The SAS 70 is intended to be a communication between the service organization auditor and the user organization auditor. A SAS 70 opinion specifically states that “This report is intended solely for the information and use of the management of service organization, its user organizations, and the independent auditors of its user organizations, and is not intended to be, and should not be, used by anyone other than these specified parties.”

The Shared Assessments AUP report is a communication from the auditor to the client, reporting the results of performing the Shared Assessments AUP. Any other party receiving the report must agree that the procedures are sufficient for their particular purposes. Many service providers request formal documentation of this agreement. The report contains language identical to the SAS 70 restricted use language (see preceding paragraph), except that it specifically identifies the intended recipients of the report.

Q Is the Shared Assessments Program replacing the SAS 70?

- A The Shared Assessments AUP process is not intended to replace SAS 70 examinations. Both the SAS 70 and the AUP were designed with a particular purpose in mind. In fact, they may be considered complementary.

Because of the SAS 70's intended purpose, financial institutions and regulators were generally not satisfied with the extent of testing performed on logical security controls found in most SAS 70 examinations. The majority of the Shared Assessments procedures are focused on logical security controls because this was the primary driver in the development of the initial set of procedures. Additionally, Shared Assessments AUP reports were designed to pass along individual test results so that those results could be evaluated in the context of each firm's unique risk control environment.

SAS 70 reports include significantly more data about a service provider's IT controls than Shared Assessments AUP reports. For many SEC companies, SAS 70 reports are the primary mechanism in obtaining information on the COSO elements and control activities in place at their service organizations. Unless the current regulatory standards change, this information will still need to be obtained by the SAS 70 user organizations' financial statement auditors.

Q Should the SAS 70 and the Shared Assessments AUP be performed together?

- A A SAS 70 examination and a Shared Assessments AUP may be performed at the same time. In certain situations, the scope of each engagement may overlap significantly. In these situations, the service provider may realize significant economies by performing the two simultaneously, using the same resources.

The Shared Assessments AUP report is often viewed as complementary to a SAS 70 report. The Shared Assessments AUP generally provides more detail on the results of the procedures performed. For example, in a SAS 70 examination procedure, a company might typically obtain and read the security policy. Shared Assessments AUP Procedure B.2 calls for the auditor to obtain the security policy and document the approval and date of the last modification. The additional effort to inspect evidence of approval (e.g., review minutes of the meeting of the steering committee approving the policy) would likely be minimal.

If the client is primarily concerned with logical security controls, then a Shared Assessments report alone may be sufficient. This may be the case if the auditor of a user organization has determined that a SAS 70 report is not required for his or her purposes.

In addition, a Shared Assessments AUP engagement may be performed in essentially any information systems environment, regardless of its purpose. A SAS 70 examination, must, however, be tied to a system or process that is part of the financial information system of the user organizations.

Q Do I really need both? Couldn't I simply incorporate the Shared Assessments Program procedures into my SAS 70?

- A Shared Assessments AUP procedures may be incorporated into a SAS 70 if the systems and infrastructure covered by the Shared Assessments AUP are appropriate to include in the scope of the SAS 70 (e.g., if they are relevant to the financial statement assertions of the user organization). However, not all procedures are appropriate for inclusion in a SAS 70. For example, Shared Assessments AUP Procedures K.1 and K.2 address Business Continuity Management, which is out of scope in a SAS 70 engagement.

Service provider organizations should compare the content of the two reports to determine if it benefits the reader to combine the two. Combining the two reports could mislead the reader or otherwise detract from the readability of the report. By keeping the reports separate, a user may more quickly assess the results of the Shared Assessments AUP.



The Shared Assessments Program thanks the authors of this document

Niall Browne, Director of Information Security, Yodlee Inc.
Andy Hout, Information Security Officer, Citi
Eddie E. Holt, Partner, KPMG LLP
Gary Roboff, Senior Consultant, BITS and The Santa Fe Group

About the Shared Assessments Program

Launched in February 2006, the Shared Assessments Program was founded by BITS member financial institutions. The program is improving the service provider assessment process by introducing common-sense efficiencies and cost savings while raising the bar on security across the industry. The Shared Assessments Program documents are updated periodically and are available for free download at www.bitsinfo.org/fisap. The Shared Assessments Program is managed by The Santa Fe Group (www.santa-fe-group.com).

About BITS

BITS was created in 1996 to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. A division of The Financial Services Roundtable, BITS works to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. BITS provides intellectual capital and addresses emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS' efforts involve representatives from throughout our member institutions, including CEOs, CIOs, CISOs, and fraud, compliance and vendor management specialists.

About The Santa Fe Group

The Santa Fe Group (www.santa-fe-group.com) is a strategic partner and preferred provider to BITS. The Santa Fe Group is a strategic consulting company providing expertise to clients on information security strategy, fraud reduction, payments strategies, innovation and emerging technologies. Drawing from the most advanced thinking in the industry, a national network of technology and security experts, and our deep knowledge of industry regulatory and legislative issues, we bring outstanding results to our clients.