



What are SSAE No. 18s and How Do I Use Them?

Background

All Reporting Entities engage Service Organizations to perform services on their behalf, such as processing payroll. Service Organizations that want to provide their customers (and their auditors) with a level of assurance that they have strong internal controls in place over the services they provide for their customers hire auditors to perform a Statements on Standards for Attestation Engagements (SSAE) No. 18 examination.

What is an SSAE No. 18 Report?

The examination results in a System and Organization Controls (SOC) report. These reports summarize the processes and controls in place to completely and accurately process transactions on customers' behalf. For example, the Defense Finance and Accounting Service (DFAS) has an SSAE No. 18 report over the systems and processes it uses to process civilian payroll for its customers.

There are three different types of System and Organization Controls (SOC) reports that can be issued under a SSAE No. 18 examination. A SOC 1 Report, known as a Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting, is the most commonly used. There are two types of SOC 1 reports:

- Type 1 – is a report confirming that the Service Organization's management has accurately described its controls, as well as the auditor's assessment on the design of those controls (but does not include any testing of whether these controls are operating effectively)
- Type 2 – is a report confirming that the Service Organization's management has accurately described its controls, as well as the auditor's assessment on the design AND operating effectiveness of those controls

SSAE No. 18 SOC 1 Type 1 reporting is seen merely as a starting point for service organizations, with the ultimate goal of undertaking SSAE No. 18 SOC 1 Type 2 reporting procedures.

How Do I Use an SSAE No. 18 Report?

The basic uses of the SSAE No. 18 Report include:

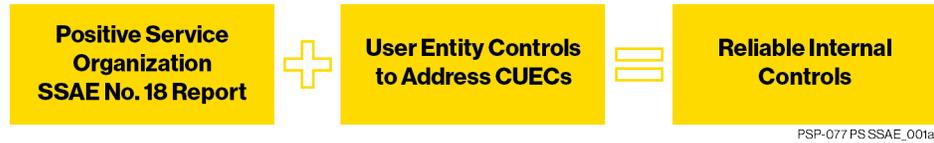
- Allowing user entities to obtain an understanding of the Service Organization's operations.
- Allowing user entities to obtain an understanding of the design/operating effectiveness of Service Organization controls.
- Minimizing redundant testing of Service Organization controls by user entities and their financial statement auditors.

The SSAE No. 18 Report has four (sometimes five) sections:

1. Independent Auditor's Report – Includes the Auditor's Opinion on the design and operating effectiveness of controls and their ability to meet the control objective.
2. Management's Assertion – Service Organization Management's written assertion that the Service Organization's system was designed, implemented, and operated effectively throughout the specified period.
3. Management's Description of Systems – Contains aspects of the Service Organization's control environment, risk assessment, information and communication, monitoring of controls, and control activities that may impact the services provided to user entities. This section may also include control objectives and related controls, description of information technology systems and controls narratives, and complementary user entity controls.
4. Control Objectives, Controls, and Test Results – Lists the control objectives, control activities, types of tests performed by the independent auditor, and results of the tests performed by the independent auditor.
5. Other Information Provided by Management – Includes additional information which the Service Organization may desire to include in the report that are not included within the scope of the audit opinion (e.g., business continuity/disaster recovery planning).

What are Complementary User Entity Controls (CUECs)?

CUECs are the specific areas that the Service Organization identifies in the SSAE No. 18 Report as the customer's responsibility in order for the Service Organization controls described in the SSAE No. 18 Report to be effective. User Entities wanting to use the SSAE No. 18 Report must ensure they have internal controls in place to address each CUEC.



How Does a User Entity Address CUECs?

The User Entity reviews the CUECs identified in the SSAE No. 18 report and determines if any are applicable to them. For those that are applicable, the User Entity will need to ensure controls are in place to address the CUECs and perform testing to ensure the controls are operating effectively. For any controls that are not operating effectively, the User Entity will need to develop and implement corrective action plans. See below for an example.

CUEC Example	"User entity staff access to the Pay System has been duly authorized by an appropriate member of user entity management."
Example of User Entity Control for this CUEC	Prior to submitting user access requests to Pay System, User Entity Management reviews and signs off on completed user access request forms for all User Entity staff to ensure requests are complete, accurate, and appropriate.

What are Sub-Service Organizations?

Sub-service organizations are service organizations used by another service organization to perform some of the services provided to user entities that are relevant to those user entities' internal controls. User entities need to know that the right processes and controls are properly designed and implemented not only at their service organizations, but also at subservice organizations. User entities should request a copy of the SOC 1 report from the subservice organizations named in the scope section of the service organization's SOC 1 report.

How can Guidehouse Help?

Guidehouse has advised civilian and defense agencies regarding SSAE No. 18s and the development of CUECs. For example, at the DOD Guidehouse developed a master spreadsheet of containing all CUECs from all of the Department's SOC 1 Reports, including baseline control descriptions, examples of key supporting documentation, and sample test procedures to be used by management to test the design and operating effectiveness of the CUE Cs. From a Reporting Entity perspective, PwC has used the spreadsheet to help ensure that all appropriate controls have been designed and implemented at their organization. From a User Entity perspective, PwC has used the spreadsheet to help entities ensure that they have carefully analyzed the SOC 1 Reports that they use, and to ensure that they have implemented appropriate CUECs.

For more information,
please contact:

Craig Atkinson
Managing Director
(540) 454-8760
catkinson@guidehouse.com

Bradley Keith
Director
(804) 304-7005
bkeith@guidehouse.com

 Follow us on Twitter
@guidehouse_us