Williams Overman Pierce, LLP
Certified Public Accountants and Consultants

Building Trust in Cloud Services—The SOC Standard

As cloud computing service models continue to be adopted as cost-effective, efficient technology solutions, customers of such companies are demanding high levels of assurance from service providers about the integrity, accuracy and reliability of the services provided to them—especially when sensitive financial, private and confidential data are involved. Such assurance is critical for risk management and mitigation at user entities, which retain responsibility for any outsourced services.

In highly regulated industries like financial services, third-party compliance isn't a nice-to-have; it's a must-have. The Consumer Financial Protection Bureau, the Office of the Comptroller of Currency (OCC), and other regulators have shared explicit examination guidance on third-party risk management. The OCC actually mandates that banks stipulate the types and frequency of audit reports required in contracts with third parties. Similarly, in the healthcare industry, business associates and subcontractors are held liable under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security and Privacy rule. As a result, companies that provide cloud services in financial services or healthcare industries are also impacted by those contractual and/or regulatory requirements.

Cloud service providers can offer their clients the expected assurance through Service Organization Control (SOC) reports. These attestations focus on the design and operating effectiveness of controls related to financial reporting or operational controls at service organizations. SOC reports have become the market standard for third-party attestations, and can serve as a powerful testament to a company's commitment to sound operating practices and its ability to meet regulatory and internal controls compliance, as well as market demands. SOC is increasingly becoming a necessary prerequisite to advance in the sales discovery and request for proposal (RFP) processes.

What follows is a guide to the SOC 1, SOC 2, SOC 2+ and SOC 3 reports, the differences between Type 1 and Type 2 reports, the benefits of these reports and how to prepare for them.

Benefits of SOC for Cloud Service Providers

Undertaking SOC attestation can provide numerous benefits, including building trust with current customers and prospects. SOC reports provide a look under the hood without requiring the user entity to perform the audit itself. Most large organizations partner with hundreds or even thousands of outside service providers, and auditing each vendor one-by-one would be time-consuming, inefficient and disruptive to both parties. Similarly, cloud computing is a volume business; permitting each user entity to perform its own audit with different criteria and reporting simply isn't feasible from a time or cost perspective.

Public companies, which must answer to both investors and regulators, may be more likely to engage a cloud service provider for outside services if the service provider has met the rigors of the SOC process. However, private companies are also seeking higher levels of assurance from their vendors, particularly those they rely on to store, process and transfer either their own or their customers' data. SOC reports can also be a factor in the RFP process—some companies demand them as a condition of participating.

Other company stakeholders and prospective investors look for SOC attestation, especially from private technology companies, as a good measure of corporate health when they contemplate or plan an exit strategy, such as an initial public offering (IPO) or a sale to a strategic buyer. Companies inherit the risk of their target following an acquisition, and many include SOC queries in their due diligence.

Finally, having a third party examine a cloud service provider's controls and activities provides peace of mind about whether the controls are functioning as expected, and how they can be improved. At the very best, going through the SOC process is a visible sign of "good health." At its worst, it can indicate where and when there are breakdowns in the controls that could possibly lead to fraud or other problems so the organization can address them as soon as they are identified.

SOC 1 Reports

SOC 1 reports on controls at a service organization relevant to user entities' internal control over financial reporting (ICFR). In other words, SOC 1 focuses on the controls established by a third party (i.e., cloud service providers, known as "service organizations") that are pertinent to the financial reporting of its clients (known as "user entities"). When moving to the cloud, companies generally use a third-party service provider that processes or retains physical and/or logical access to user entities' data. To the extent the services provided by the service organization impact the user entities' internal controls over financial reporting, moving to the cloud is likely to have financial reporting implications for user entities. Prepared in accordance with Statement on Standards for Attestation Engagement (SSAE) No. 16/ AT 801 (SSAE 18, AT-C Section 320 for reports dated on and after May 1, 2017), the SOC 1 report is intended to meet the needs of user entities and the auditors of user entities' financial statements.

A completed SOC 1 report shows that an independent service auditor (i.e., a CPA) performed an examination of the service organization's procedures—both automated and manual—including transaction processing and information technology controls relevant to user entities' ICFR, associated with the services provided. SOC 1 reports should be used only by the management of service organizations, users of the service organization's services (i.e., user entities) and the user entities' financial statement auditors.

The SSAE 16 standard, which replaced Statement on Auditing Standards (SAS) No. 70, requires that the management of the service organization assume responsibility for making certain assertions. In SOC 1 reporting, management must assert that:

- The description fairly presents the system made available to user entities of the system as of a specific date for a Type 1 report or throughout a period of time for a Type 2 report.
- The controls related to the control objectives stated in management's description were suitably designed and implemented as of a specific date for a Type 1 report or throughout a period of time for a Type 2 report to achieve those control objectives (and those controls were operating effectively to achieve the stated control objectives in a Type 2 report).

The service auditor performs SOC 1 examination procedures to provide an opinion on the following based on the criteria described in management's assertion that:

- The description fairly presents the system that was designed and implemented as of a specific date for a Type 1 report or throughout a period of time for a Type 2 report.
- The controls related to the control objectives stated in management's description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively as of a specific date for a Type 1 report or throughout a period of time for a Type 2 report.
- The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout a period in a Type 2 report.

Furthermore, if the service organization relies on another organization (i.e., a subservice organization) to perform any of the related services, the service organization must delineate in its SOC report whether the subservice organization's controls are excluded from the service organization's report (i.e., a carve-out approach) or included in the service organization's report (i.e., an inclusive approach). If the service organization issues an inclusive report, the report must include an assertion from the subservice organization's management, similar to that from the service organization's management. Under the inclusive approach, the service auditor performs the examination procedures to provide an opinion, similar to the procedures performed at the service organization, related to the subservice organization's controls that are included in the SOC report.

SOC 2, SOC 2+ and SOC 3

As cybersecurity rises to the top of the risk management agenda, user entities are increasingly seeking additional assurance of non-financial controls pertaining to systems and data privacy, confidentiality, availability, processing integrity and security. The AICPA is expected to issue guidance specifically related to cybersecurity within the next year.

In the meantime, companies are contending with increased concerns over data security through the issuance of SOC 2, SOC 3, and/or SOC 2+ (SOC 2 principle(s) plus cloud security, HIPAA criteria, etc.) reports. These reports attest to the controls around systems and data privacy, confidentiality, availability, processing integrity and security, depending on which principle the report covers.

SOC 2, SOC 2+, and SOC 3 reports are examination engagements performed by a CPA in accordance with AT Section 101, *Attest Engagements*, of SSAEs (AICPA, *Professional Standards*). These reports are to be performed in accordance with SSAE 18, AT-C Section 205, for reports dated on and after May 1, 2017.

SOC 2 and SOC 3 reports are issued to meet predefined criteria for one or more of the trust services principles set forth in TSP section 100, Trust Services Principles, Criteria and Illustrations for Security, Availability, Processing Integrity, Confidentiality and Privacy (AICPA, Technical Practice Aids). The AICPA has provided specific guidance in performing SOC 2 reports, and these reports are performed using the AICPA Guide: *Reporting on Controls at a Service Organizations Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy*. SOC 2 and SOC 3 reports specifically address one or more of the following five key system attributes:

1. **Security** - The system is protected against unauthorized access (both physical and logical);
2. **Availability** - The system is available for operation and use as committed or agreed;
3. **Processing integrity** - System processing is complete, accurate, timely and authorized;
4. **Confidentiality**-Information designated as confidential is protected as committed or agreed;
5. **Privacy** - Personal information is collected, used, retained, disclosed and disposed of in conformity with the commitments in the entity's privacy notice, and with criteria set forth in Generally Accepted Privacy Principles (GAPP) issued by the AICPA and CPA Canada [The criteria in GAPP are the same as the criteria for the privacy principle in TSP section 100].

SOC 2 can prove useful in organizational and regulatory oversight, vendor management, and governance and risk management endeavors. The SOC 2 report contains a detailed description of test of controls performed by the service auditor, along with the results of those tests, auditor's opinion and the service organization's description of the system. SOC 2 can also be adapted to evaluate additional subject matter related to the service organization's services using additional suitable criteria related to that subject matter, such as industry-specific criteria, on top of the applicable trust services principles. Of note, the Cloud Security Alliance developed the Cloud Control Matrix. Similarly, the Health Information Trust (HITRUST) Alliance—the organization responsible for the development of the HITRUST Common Security Framework (CSF)—and the AICPA collaborated to develop and publish a set of recommendations to streamline the process of leveraging the HITRUST CSF for SOC 2+ reporting. Likewise, a service organization may also want to report on additional criteria to address requirements set forth in the HIPAA Administrative Simplification 45 CFR Sections 164.308-316.

When a service organization wants a report on both the trust services principles and the additional criteria—such as the HITRUST CSF, the Cloud Controls Matrix from the Cloud Security Alliance, etc.—a SOC 2+ report is an option. A SOC 2+ report provides the service organization with a service auditor's examination report that includes:

- An opinion on the fairness of the presentation of the description based on the description criteria in the AICPA SOC 2 guide, and
- An opinion on the suitability of the design of controls for a Type 1 report (and operating effectiveness of the controls for a Type 2 report) based on:
    - The applicable trust services criteria, and
    - The additional criteria applicable to the organization, such as HITRUST CSF requirements, HIPAA regulatory requirements, the Cloud Security Alliance's Cloud Control Matrix, etc.

SOC 3 is a general-use report which reports on the suitability of design and the operating effectiveness of an entity's controls over a system relevant to one or more of the trust services principles. In contrast to the SOC 2, there are no detailed descriptions of tests of controls performed by the service auditor and results of those tests in a SOC 3 report. SOC 3 reports cover a period of time. Both SOC 2 and SOC 3 can be issued on one or more of the trust services principles.

Similar to SOC 1 reports, the service organization's management is responsible for making management assertions in SOC 2 and SOC 3 reports.

Type 1 and Type 2 Reports

Both the SOC 1 and SOC 2 attestations provide two types of report options: Type 1 and Type 2. A Type 1 report considers the design and implementation of controls and their suitability to meet the specified objectives in case of a SOC 1 report or applicable trust services criteria in case of a SOC 2 report at a single point in time (a specified date). A Type 2 report also considers the operating effectiveness of those controls over a specified period of time and will include the service auditors' tests of controls and the results of those tests. A Type 1 SOC 1 or SOC 2 engagement addresses the same subject matter as a Type 2 SOC 1 or SOC 2 engagement, respectively; however, a Type 1 report does not contain an opinion on the operating effectiveness of controls, nor a detailed description of tests of controls performed by the service auditor, and results of those tests.

If your organization performs outsourced services that affect the internal controls over financial reporting of a user entity, it is likely you will be asked to provide a SOC 1 Type 2 report, especially if the user entity is a publicly traded company.

If your organization performs outsourced services that affect systems and data security, availability, confidentiality, processing integrity or privacy-related controls of a user entity, it is likely you will be asked to provide a SOC 2 Type 2 report. If the outsourced services affect both the internal controls over financial reporting as well as systems and data security, availability, confidentiality, processing integrity or privacy related controls of a user entity, the growing trend is that both SOC 1 and SOC 2 reports will be requested from the service organization.

In our experience, most user entities will require a Type 2 report before contracting with a cloud service organization (user entities generally accept a Type 1 report in year one, and expect a Type 2 report from year two onward).

Access and Use

Intended as an auditor-to-auditor communication, use of the SOC 1 report is restricted to management, the service organization's clients and the clients' financial statement auditors. In addition to these parties, a SOC 2 report may be distributed to appropriate business partners, prospective customers, vendor management executives and regulators. Distribution and use of a SOC 3 report is generally unrestricted.

Getting Ready for SOC

When should you get a SOC report? Service organizations frequently wait until it is requested or required of them. However, bear in mind that SOC reports can take as long as six months to a year to prepare for. In addition, most clients (user entities) prefer the SOC attestation to have been performed within the last six months to a year. From the Public Company Accounting Oversight Board's perspective, a SOC 1 report that is more than three months old is a potential issue unless a gap letter (also known as a bridge letter) is obtained for the period not covered by the SOC report. Once an organization completes its first SOC examination, reports are typically performed on an annual basis going forward, but more frequency may be necessary.

The most critical considerations before undertaking a SOC examination are determining which type of SOC report is most appropriate (SOC 1 or SOC 2, SOC 2+ or SOC 3), what control objectives or trust services criteria are most relevant, and the scope of the audit. Certain internal systems may not have any impact on the services provided to the user entity, and can be excluded from the report.

Before engaging with a SOC auditor, organizations should review their policies and procedures, how they are documented, communicated and enforced, and conduct their own internal testing. Most organizations opt to do a "pre-assessment" prior to the actual examination. The goal of the pre-assessment is to identify and remediate any gaps before the formal SOC audit to prepare for a favorable SOC report.

Early-stage companies can get a head start by designing software, processes and controls with an eye toward eventually undergoing the SOC attestation. It is easier to implement the controls initiative from the beginning rather than implement them after the fact.

What to Expect

A SOC report will contain the auditor’s opinion about the following aspects of a service organization’s controls:

- Whether the description of controls is presented fairly
- Whether the controls are designed and implemented effectively
- Whether the controls are operating effectively over a specified period of time (only in a Type 2 report)

If the auditor finds the objectives listed above have been achieved by the service organization, the service auditor will issue an “unqualified” opinion. If exceptions noted in the examination are limited to one or more, but not all, aspects of the description of the service organization’s system or control objectives, the auditor considers a need to issue a “qualified opinion.”