APPLYING THE SOC FRAMEWORK TO DIGITAL ASSETS

Ria Bhutoria, Director of Research

The adoption of the SOC reporting framework by digital asset service providers speaks to the industry's maturation and belief in providing strong, standardized assurances and transparency to stakeholders.

Introduction

In the traditional financial services industry, third-party service providers such as custodians, exchanges and fund administrators leverage SOC (System and Organization Controls)[i] reports to build stakeholder trust and confidence. SOC reports are internal control evaluations conducted by independent auditors. The interest in attaining SOC reports has been driven by the recognition that the reports disclose important information about third-party provider controls that end-users need to comprehensively assess and address the risks of outsourced core services. Thus, the adoption of the universal SOC reporting standard by digital asset service providers speaks to the industry's maturation and belief in providing stronger and more standardized assurances and transparency to stakeholders.

Independent audit firms (known as service auditors) perform SOC examinations on companies (service organizations) based on guidelines established by the American Institute of Certified Public Accountants (AICPA). SOC examinations are tests of internal controls and processes that impact an organization's end users. AICPA's SOC reporting framework presents three reporting options. The types of services and systems a company offers along with user-specific needs informs the type and scope of audit an organization should obtain. In this piece, we explain the differences between the main reports, and how these reports apply to digital asset service providers.

Terminology

Before going further, we'd like to define certain key terms in the context of SOC reports given significant SOC report specific terminology.

1. **Service organization:** A service organization is the subject of a SOC report. It is a company to which customers outsource critical services. Exchanges, custodians, cloud providers and software-as-a-service companies (e.g. AWS) are common examples of service organizations. We use service organization and service provider interchangeably in this piece.
2. **Service auditor:** An independent CPA firm that conducts analysis and testing to assess the reliability of a service organization's systems. Service auditors develop opinions on the service organization's design of internal controls (provided in Type I and Type II reports) and the operating effectiveness of internal controls in meeting the objectives (provided in a Type II report) based on this testing and analysis.
3. **User entity:** A user entity is the customer or client of a service organization that seeks assurances about its service organizations. User entities request SOC reports from their service organizations. We use client, customer, and user entity interchangeably in this piece.
4. **Control objective:** A control objective articulates the aim or purpose of a specified set of processes at a service organization. Control objectives should be relevant to services offered to customers.
5. **Controls**: Controls are internal activities performed by a service organization, An auditor evaluates a set of controls to determine if the respective control objective has been met.
6. **Trust services categories**: Trust service categories are areas of focus in SOC 2 reports. The five categories are security, availability, processing integrity, confidentiality and privacy. A SOC 2 report may include multiple categories.
7. **Trust services criteria:** Evaluation criteria that can be used to determine the suitability of the design of a service provider's systems and the operating effectiveness of controls relevant to the trust services category being assesses.
8. **SSAE 18:** Standards developed by the AICPA for use by service auditors against which to evaluate internal controls at service organizations.
9. **AT Section 320:** This is a sub-section of SSAE 18 that is relevant to SOC 1 reports.
10. **AT Section 105:** This is a sub-section of SSAE 18 that is relevant to SOC 2 and 3 reports.
11. **AT Section 205:** This is a sub-section of SSAE 18 that is relevant to SOC 2 and 3 reports.

The Emergence of SOC Reports

The growth in outsourcing critical financial and IT functions to specialized organizations has fueled the development of the standardized SOC system for evaluating internal controls. The AICPA introduced the SOC reporting framework in 2011 to refresh older standards (specifically SAS 70) and expand the subject matter covered by internal control audits.

The updated SOC framework provides standardized audit options to the evolving landscape of service organizations and reconciles with international accounting standards (specifically, ISAE 3402).[ii] The updated framework consists of SOC 1, SOC 2 and SOC 3 reports that are prepared in accordance with sub-sections of the AICPA's audit standards, known as the Statement on Standards for Attestation Engagements No. 18 (SSAE 18).

SOC 1 reports broadly comment on controls and processes that impact user entity financial statements and reporting. SOC 2 reports comment on controls and processes that address the security, availability and/or processing integrity of systems and/or confidentiality, privacy data. A SOC 3 report is a condensed, less detailed version of a SOC 2 report.

SOC Reporting Requirements

While service organizations are generally not required by law to undergo SOC audits, one of the main reasons for enlisting an audit firm to issue a SOC report is that user entities are increasingly demanding such internal control reports from their outsourced-service providers. One way this has manifested is via contractual terms between a service organization and its clients that require the service organization to engage independent auditors regularly to conduct SOC audits.

Type I vs. Type II

SOC 1 and 2 reports can be sub-categorized into Type I and Type II reports. A Type I report is an attestation of controls at a service organization at a specific point in time, whereas a Type II report is an attestation of controls at a service organization over a minimum six-month period. A Type I report contains the auditor's opinion on the fairness of the design of internal controls. Type II reports are generally more comprehensive as they incrementally include the auditor's opinion on the operating effectiveness of the controls over the audit period and a detailed account of the tests the auditor performed and the results of the tests.

Components of SOC Reports

In SOC 1 and SOC 2 Type I reports, the service auditor outlines the scope of the audit, the responsibilities of the service organization and auditor in the audit process and an opinion on the design of the system and controls at a specific point in time. In SOC 1 and SOC 2 Type II reports, the service auditor outlines the scope of the audit, the responsibilities of the service organization and auditor in the audit process, the limitations of the audit, the outcome of the tests, the provider's effectiveness in achieving the objectives and the auditor's final opinion based on the results of the tests – i.e. do all activities, taken together, achieve the objectives – over a period of time.

The management of the service organization also contributes to the report. Specifically, management provides a description of its systems and the assertions it is making about the systems. The description includes the chosen control objectives (SOC 1) or categories and corresponding criteria (SOC 2) and the control activities. Management may also provide other information such as about controls that the audit does not cover and a response to the auditor's opinion and exceptions.

SOC 1	SOC 2
Auditors opinion	Auditors opinion
Management assertion	Managemant assertion
Description of system and controls	Description of system and controls
Control objectives	Trust services categories and criteria
Auditor's tests of controls*	Auditors tests of controls*
Auditor's results of tests*	Auditor's results of tests*
Other information	Other information

Source: PwC

**Type II reports only*

Initial SOC engagement

There are four distinct phases in an initial SOC engagement – the initial conversation between firm and auditor, the readiness assessment, remediation, and reporting. In the initial conversation, auditor and service provider determine the appropriate report and scope. The service auditor then performs a readiness assessment to identify areas that require attention and remediation in advance of the audit. The following remediation period gives the organization a chance to address any potential gaps highlighted by the auditor. The audit ensues. A service organization will usually engage an auditor to produce a Type I report before the deeper Type II engagement.

SOC 1 Reporting

SOC 1 reports cover service organization activities that impact the financial statements of their user entities (the customers or clients of the service organization). SOC 1 reports are important tools that user auditors (auditors of user entities) leverage when evaluating assertions made by user entities in their financial statements. For example, a user auditor may look to the SOC 1 of the user's custodian for assurances that the digital assets listed on the user entity's balance sheet exist and belong to the client.

A service organization can choose a single line of business (e.g. custody or trading) to audit or choose an enterprise-wide audit of all business lines simultaneously. A user entity that relies on a service organization for multiple services should check whether one or all services have undergone an audit.
SOC 1 reports are prepared in accordance with evaluation standards established by the AICPA. SSAE 18, a set of standards created by the AICPA, governs all SOC reports. The section of SSAE 18 that pertains to SOC 1 reports is AT-C Section 320 (Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting) of SSAE 18.

SOC 1 audits evaluate the design of control objectives defined by service organizations and test the operational effectiveness of controls in achieving the objectives. A control objective is a target against which the effectiveness of controls (i.e. activities the service organization performs) is evaluated.[iii] SOC 1 reports are primarily designed for and consumed by auditors of user entities. However, other stakeholders who may be interested in the contents of SOC 1 reports could include investors allocating to funds that use service providers (e.g. custodians, exchanges, fund administrators) or businesses that are considered partners of the service organization.

Traditional and digital asset service provider controls

The AICPA shares illustrative control objectives that apply to many types of organizations. It also publishes illustrative control objectives for specific types of service organizations (e.g. custodians, investment managers, transfer agents). Although the AICPA has yet to define illustrative objectives specific to the digital assets industry, service providers in the space and their auditors may use the illustrative objectives from traditional industries as a starting point to develop a comprehensive control framework specific to the service provider. Actual objectives can vary since the illustrative objectives are only meant to serve as a guide.

A digital asset custodian will define similar overarching control objectives as their legacy custody counterparts. A SOC 1 audit tests controls around how assets are moved to and from the custody environment, how the custodian documents client account information, how client transactions (e.g. contributions, trades and withdrawals) are processed and booked, how digital assets are reconciled to the custodian's books and records, and how the custodian restricts access of personnel to assets and how it safeguards assets from loss or misappropriation.[iv] It is also standard practice for custodians to have reconciliation related objectives in their SOC 1 reports. For a digital asset custodian or exchange, a reconciliation control would, more specifically, confirm at regular intervals that assets held on-chain match assets owed to clients (customer accounts off-chain).

Reconciliation could be compared to testing controls around internal proof of reserves. Proof of reserves has been a frequent topic of conversation in the industry given substantial funds lost as a result of exchange hacks and exit scams. While SOC 1 reports do not establish a proof outright, they may provide greater confidence that the service provider has reconciliation practices that an independent auditor believes are reliable. In a SOC 1 report, a traditional custodian may also outline a control objective around executing a wire transfer. The parallel for a digital asset custodian would be the test of controls related to on-chain transfers.

Processes that are unique to digital asset service providers include key generation and management. Key generation, management and safekeeping are critical functions for digital asset service providers given ownership is designated by private keys and digital assets are bearer instruments (like physical cash). Whoever has access to the private key associated with digital assets can control the assets. Losing the private key results in the irreversible loss of assets associated with the private key. Thus, there is an

enhanced need for logical controls around digital assets and digital asset transactions relative to legacy financial securities given there is no DTCC-parallel that can recover the assets. SOC 2 audits may test similar controls.

A correctly scoped SOC 1 audit will also include incremental technology controls that need to be evaluated to achieve financial reporting control objectives. As a result, a significant portion of controls tested in a SOC 2 report on security and/or processing integrity may also be tested in a robust SOC 1 audit. We detail security-related procedures that may be tested in sections below.

Applicability of SOC 1 to digital asset industry

It is important for digital asset service organizations that impact the externally audited financial statements of customers to obtain SOC 1 reports. Digital asset custodians and exchanges fall into this category and should offer their clients and clients' auditors SOC 1 reports. The AICPA explicitly says that custodians for investment companies provide services that are relevant to user entities' financial reporting because they are "responsible for the receipt, delivery, and safekeeping of an investment company's portfolio of securities; the receipt and disbursement of cash resulting from transactions in these securities; and the maintenance of records of the securities held for the investment company."[v]

Any company or fund (i.e. any user entity) that has digital assets on its balance sheet and/or within its revenue stream as well as externally audited financial statements needs financial services and custody providers (i.e. service organizations) that regularly procure SOC 1 reports. The financial statement auditors of user entities (i.e. user auditors) are key stakeholders that expect their clients to select service providers that provide SOC 1 reports. Other stakeholders interested in SOC 1 reports may include internal audit and risk management teams, business partners or regulators of the service providers and their user entities. SOC 2 reports do not satisfy the requirements of these stakeholders.

SOC 2 Reporting

Generally, a SOC 2 attestation evaluates a service provider's controls over client information and systems that store and process the information (vs. a SOC 1, which covers financial reporting such as controls related to client assets and systems that maintain and process the assets). SOC 2 audits are performed in accordance with different sub-sections (AT-C Section 205 and AT-C Section 105) of the AICPA's standards related to SOC reporting (SSAE 18). As a reminder, SSAE 18 establishes audit guidelines, which auditors must adhere to when performing SOC audits to ensure that service organizations are evaluated based on consistent standards and criteria.

SOC 2 reports have become more common with the growth in sensitive data transmitted and stored online and firms outsourcing tasks or entire functions to specialized businesses. By issuing a SOC 2 report, firms that have access to sensitive data can offer stakeholders assurances around the data and "help them satisfy their vendor management, business continuity or regulatory requirements." The intended audience of SOC 2 reports are the service organization user entities, their internal auditors and compliance personnel and regulators that understand the service provider's business.[vi]

SOC 2 audits are becoming a standard practice for firms providing cloud storage, software-as-a-service, data processing and other technology-related services in traditional technology and finance industries, as stakeholders demand assurances around customer data protection processes and safeguards. SOC 2 audits cover a service provider's IT-related operational and compliance controls that correspond to the AICPA's trust services categories – security, availability, processing integrity, confidentiality and privacy. At a minimum, all SOC 2 reports must contain the evaluation of controls related to security. The selection of additional categories is optional and depends on the applicability the service organization's systems and services.[vii]

- **Security:** The system is protected against unauthorized access (both physical and logical). Fully-scoped SOC 1 reports should also include tests of physical and logical security controls.
- **Availability:** The system is available for operation and use as committed or agreed.
- **Processing integrity:** System processing is complete, accurate, timely and authorized. Robust SOC 1 audits will also cover processing integrity related procedures, as they are important to timely financial reporting.
- **Confidentiality:** Information designated as confidential is protected as committed or agreed.

- **Privacy:** Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set in generally accepted privacy principles (GAPP).

The criteria associated with security is referred to as the "common criteria" because it applies to all five categories. The common criteria comprise the complete set of criteria that pertains to security. Availability, processing integrity, confidentiality and privacy have additional criteria that are specific to those categories. In order to meet the requirements of SOC 2 reporting, service organizations must address each of the common criteria as well as additional criteria associated with the non-security categories they may include. AICPA divides the set of common criteria (thirty-three in total) across nine buckets: Control environment, Communication and information, Risk assessment, Monitoring activities, Control activities, Logical and physical access controls, System operations, Change management, Risk mitigations.[viii]

Traditional and digital asset service provider controls

Each category has corresponding trust services criteria. A service organization must achieve each criterion within a category to satisfy the category requirements. "Points of focus" under each criterion guide the selection, design, implementation and evaluation of controls.[ix] Points of focus are akin to the illustrative controls that guide SOC 1 evaluations. SOC 2 reports are relatively standardized compared to SOC 1 reports given the predefined trust services categories and criteria. However, the AICPA has yet to publish standardized guidelines for service providers in the digital asset space.

SOC 2 reports test a variety of tech-oriented controls related to the trust services categories. At a high level, SOC 2 reports opine on whether transactions, assets and data are secure and protected. An auditor performing a SOC 2 examination around security may test controls related to security monitoring and compliance, the communication of security risks and policies and user administration and authentication. Additional controls related to an optional category, such as privacy, could cover user consent, access to data or the use and retention of personally identifiable information of users.[x] As we mentioned above, fully-scoped SOC 1 reports will also include a large variety of these technology and security controls given they are also required to adequately meet financial reporting control objectives.

SOC 2 reports can provide peace of mind to user entities of digital asset service providers given heightened security concerns around these virtual bearer assets. SOC 2 reports for digital asset service providers such as custodians or exchanges may contain net new areas such as the security, availability or integrity of systems and processes related to the storage of the service provider's private keys and digital asset wallet configurations.

Applicability of SOC 2 to the digital asset industry

SOC 2 reports are relevant to a broad variety of third-party service organizations – the underlying thread is that service organizations handle, process and/or maintain sensitive data of their customers. Of the SOC 2 reports that PricewaterhouseCooper (PwC) issued in 2018, 49% of reports were issued to companies in the technology sector, 14% of reports were issued to companies in banking and capital markets and 7% of reports were issued to companies in the asset management industry.[xi]

If a SOC 1 report is not available or applicable, digital asset service providers that store and process sensitive data of end-users can leverage SOC 2 reporting to offer specific assurances. Depending on the categories covered and the opinion generated, service providers can demonstrate to stakeholders that their systems have appropriate safeguards and secure systems in place to transmit, store, maintain, process and dispose of sensitive data.

Key Considerations for User Entities

There are certain considerations to be aware of when reviewing the reports. It is not enough to know that a company has received an attestation from an audit firm. It is not enough to take the high-level opinion presented by the service auditor at face value.

Is it a SOC 1 or SOC 2 report? Clients should ensure their service organization produces reports that meet their needs, as the two reports provide different assurances. However, SOC 1 reports also contain tests of controls related to the security and/or processing integrity criteria covered in SOC 2 reports. SOC 2 reports, on the other hand, cannot provide any assurances about controls related to a user entity's financial statements.

- **Is it a Type I or Type II report?** Think of a Type I report as a "lite" attestation. A Type II report is more comprehensive as it covers a period of time and includes the service auditor's opinion on the operating effectiveness of the controls as well as a detailed account of the tests of controls and results of the tests. Service organizations and their auditors generally go on a journey, starting with the readiness assessment to Type I to Type II.
- **Is the auditor's opinion unqualified or qualified?** It is always preferable if a service provider obtains a report with an unqualified (or clean) opinion. This means that the auditor believes the system was suitably designed and there was reasonable assurance that the service provider has achieved its control objectives over the time period specified in the report based on the controls tested. If the auditor provides a qualified opinion, the auditor may have identified concerns during the reporting period that prevented the service organization from meeting its objectives.
- **Are there any exceptions related to control activities?** Stakeholders should evaluate the sections that highlight the auditors' tests and results of tests to determine whether they noted any exceptions or qualifications related to individual activities. Certain activities may be more critical for one user entity versus another.
- **Who performed the independent audit?** The quality of the audit also depends on whether the audit was performed by an established accounting firm with substantial experience and expertise or a lesser known, less experienced firm.
- **What is the timeframe of the audit?** The time period over which a SOC 1 audit took place should generally align with the user entity's fiscal year to reasonably rely on the controls being in place during the fiscal year. Otherwise, user entities and their auditors may consider reviewing consecutive SOC 1 reports.
- **Does the service auditor have expertise in the industry?** Practitioners should have adequate knowledge of the industry of the service organization they are evaluating. Firms auditing digital asset service providers should curate teams of practitioners who have relevant cybersecurity and cryptography experience to test more technical activities.

Conclusion

While SOC reports are one of many pieces in the process of vetting service providers, they establish a basis for placing trust given the relatively stronger assurances and transparency they provide stakeholders. Providers can leverage the standardized reports to assure multiple parties at once that they have implemented robust controls that meet their expectations. This prevents service providers from having to undergo one-off audits by clients, which can become operationally and financially intensive.

Simultaneously, user entities (clients of service organizations) can leverage reports to reduce their own costs of compliance. In certain cases, choosing service providers that undergo routine SOC evaluations can even help clients meet the needs of their own stakeholders, such as auditors, investors and regulators. SOC reports also provide user entities a standard framework and set of criteria to compare service providers to one another.

Undergoing a SOC audit and receiving an unqualified opinion is a significant feat. It requires developing a culture of compliance, a robust internal control and risk management system and a methodical system for collecting evidence the controls and processes are operating as intended. That may be challenging and unintuitive for new organizations to achieve and manifests in the length of the potential remediation phase after the service provider engages an audit firm to perform a readiness assessment.[xii]

In the nascent digital asset industry, the role and scope of service providers is quickly expanding (exchanges have become de-facto custodians) and the magnitude of what's at stake is unique (digital asset transactions are probabilistically irreversible). These are key reasons that the industry has suffered substantial reputational and financial damage (to the tune of $4.5 billion in losses in 2019) due to exchange hacks, fraud and misappropriation of funds.[xiii] Service providers in the space recognize that they can use SOC 1 and/or SOC 2 audits to differentiate relative to the marketplace, win the business of large established customers that expect a certain level of assurance and set higher industry standards for the status quo.

	SOC 1	SOC 2
Focus	Controls related to customer financial reporting	Controls related to system reliability
Guidance in Design	Illustrative control objectives	Trust services categories, criteria, points of focus
Control activities examples	Reconciliation Existence of assets Tx processing Asset movement Key gen. / mgmt.	Customer data storage Personnel authorization Physical / logical access Key storage Wallet software
Immediate audience	Mgmt., user auditors	Mgmt., user entity compliance, partners

Source: KPMG, PwC

SOURCES

i. https://socreports.com/white-papers/educational/aicpa-soc-reporting-framework

ii. https://kirkpatrickprice.com/video/understanding-your-soc-1-audit-report-what-are-control-objectives/

iii. https://www.aicpa.org/content/dam/aicpa/interestareas/frc/auditattest/downloadabledocuments/info-for-mgmt-of-serv-org-in-soc-engagement.pdf

iv. https://www.aicpa.org/content/dam/aicpa/interestareas/frc/auditattest/downloadabledocuments/info-for-mgmt-of-serv-org-in-soc-engagement.pdf

v. https://www.pwc.com/us/en/services/risk-assurance/third-party-assurance/soc-reporting.html

vi. https://www.pwc.com/us/en/services/risk-assurance/third-party-assurance/soc-reporting.html

vii. https://www.claconnect.com/resources/articles/2018/new-soc-report-framework-addresses-emerging-risks

viii. https://linfordco.com/blog/soc-2-security-criteria-principle/

ix. https://www.pwc.com/us/en/services/risk-assurance/third-party-assurance/soc-reporting.html

x. https://event.on24.com/eventRegistration/EventLobbyServlet?target=registration.jsp&eventid=2067568&sessionid=1&key=1D3BA3BAE729B510BEB14B8A680A72CA&sourcepage=register

xi. https://event.on24.com/eventRegistration/EventLobbyServlet?target=registration.jsp&eventid=2067568&sessionid=1&key=1D3BA3BAE729B510BEB14B8A680A72CA&sourcepage=register

xii. https://ciphertrace.com/q4-2019-cryptocurrency-anti-money-laundering-report/

ABOUT FIDELITY DIGITAL ASSETS

Fidelity Digital Assets offers a full-service enterprise-grade platform for securing, trading and supporting digital assets, such as bitcoin. Fidelity Digital Assets combines the operational and technical capabilities of the broader Fidelity organization with dedicated blockchain expertise to deliver a completely new offering for institutional investors. Fidelity Investments is one of the world's vlargest and most diversified financial services providers with more than $8.2 trillion in client assets under administration as of November 30, 2019. Learn more at fidelitydigitalassets.com.

Fidelity DIGITAL ASSETS

FIDELITYDIGITALASSETS.COM

@DIGITALASSETS

@FIDELITYDIGITALASSETS

921013.1.0