sifma®

ASSET MANAGEMENT GROUP

WHAT ASSET MANAGERS NEED TO KNOW ABOUT SOC REPORTS

JULY 2019

BDO professionals combine accounting, tax and business advisory knowledge with industry experience to help companies differentiate themselves from competitors and meet their most important goals. Backed by the resources of one of the world's largest accounting and consulting networks, BDO professionals draw their experience across multiple disciplines and sectors to provide our clients with insight, solutions and successful long term strategies.

BDO's Financial Services practice has extensive audit, tax and advisory expertise and our dedicated team possess extensive knowledge in the industry, with a deep understanding of firm structures and their overarching business implications. This allows our clients the flexibility to shift their investment strategy, knowing that BDO can adapt accordingly.

The Securities Industry and Financial Markets Association's Asset Management Group ("SIFMA AMG" or "AMG") brings the asset management community together to provide views on U.S. and global policy and to create industry best practices. SIFMA AMG's members represent U.S. and global asset management firms whose combined assets under management exceed $45 trillion. The clients of SIFMA AMG member firms include, among others, tens of millions of individual investors, registered investment companies, endowments, public and private pension funds, UCITS and private funds such as hedge funds and private equity funds. For more information, visit http://www.sifma.org/amg

TABLE OF CONTENTS

What Asset Managers Need to Know about System and Organization Controls (SOC) Reports p1

Understanding and Deriving Value from a SOC 2 Report p2

Understanding the new SOC for Cybersecurity Report p3

Comparison of SOC Reports p4

SOC Key Terms p5

WHAT ASSET MANAGERS NEED TO KNOW ABOUT SYSTEM AND ORGANIZATION CONTROLS (SOC) REPORTS

The Asset Management Group (AMG) of the Securities Industry and Financial Markets Association (SIFMA) and BDO USA, LLP, developed the following guidelines to help Asset Managers understand and leverage System and Organization Controls (SOC) reports as part of their third party/vendor risk management process. This whitepaper was developed by leveraging and applying the American Institute of Certified Public Accountants' (AICPA) 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (effective December 15, 2018), *Guide: Reporting on an Entity's Cybersecurity Risk Management Program and Controls* (May 1, 2017), *Guide: SOC 2 Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (January 1, 2018), and AICPA's Brochure *What are you doing to prevent cyberattacks?* (May 8, 2018).

In recent years, with the introduction of new privacy laws (GDPR, California Consumer Privacy Act, etc.), the Asset Management sector has been dealing with increased regulatory scrutiny focused around security, availability, processing integrity, confidentiality, and privacy surrounding customers' data.

Asset Managers are also under increased pressure to demonstrate that they are managing cybersecurity threats and have effective controls to detect, respond to, and mitigate security events.

In addition, there is increased activity related to the outsourcing of business and information technology functions, making the practice of third party risk management a major concern for many firms. Management of Asset Management firms has the ultimate responsibility to protect customer data, whether the data resides with the Asset Manager or a third party service provider. Consequently, management has a responsibility to properly research and monitor service organizations prior to onboarding, and to establish a vendor risk assessment process. The vendor risk assessment process helps management identify potential vendor risks and establish controls over the outsourced services.

Management may deploy various mechanisms in its vendor risk assessments, including audit of the third party service provider or review and evaluation of the SOC report(s) from the third party service provider. Generally, review and evaluation of the SOC report(s) is considered a more effective and efficient approach in the industry, which requires that management understands the proper use and scope of the reports received from the third party service providers.

UNDERSTANDING AND DERIVING VALUE FROM A SOC 2 REPORT

Asset Managers have become accustomed to examining the controls of service providers to fulfill financial reporting responsibilities and often review and provide SOC 1 reports focusing on internal controls over financial reporting. However, many are less familiar with other types of SOC reports available to them.

The SOC 2® - SOC for Service Organizations: Trust Services Criteria is a report on *Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy* and is intended to meet the needs of a broad range of users. Asset Managers, for example require detailed information and reasonable assurance about the controls at a service organization, such as a software provider or hosting facility, that may be relevant to security, availability, and/or processing integrity of the systems used to process Asset Managers' data and the confidentiality and/or privacy of the information processed.

In addition to a SOC 2, there is a SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report which is designed to meet the needs of users who need assurance about the controls at a service organization relevant to security, availability, processing integrity, confidentiality, and/or privacy, but do not have the need for or the knowledge necessary to make effective use of a SOC 2 Report. The SOC 3 reports can be freely distributed, but may not be as useful for evaluation of the service provider for Asset Managers.

To derive the most value from SOC 2 reports, it is important to assign responsibility to review and evaluate the reports to personnel within the Asset Manager's organization with relevant background. Since this report is less focused on controls impacting financial reporting and is more focused on technology controls, individuals such as the Chief Technology Officer (CTO), Chief Information Security Officer (CISO), Chief Information Officer (CIO), Chief Compliance Officer (CCO), or a delegee within their departments who has information security background, should be reviewing and evaluating the SOC 2 report. Asset Managers with an internal audit department should also involve the internal audit team and work with aforementioned teams to help review and evaluate these reports.

Once the appropriate reviewers are established, they should understand the scope of the report by identifying and evaluating:

- The scope and boundaries of the system being covered, which are specific aspects of infrastructure, software, people, procedures, and data necessary to provide services,
- The Trust Services Criteria in scope (Security, Availability, Confidentiality, Processing Integrity, and/or Privacy),
- The period covered by report (as of date (Type 1) or period of time (Type 2)),
- Location(s) being covered, including the data center locations, if the report is from a cloud, system or software provider,
- The subservice organizations utilized by the service organization and Complementary Subservice Organization Controls (CSOCs) listed in the report that the Asset Managers may need to obtain additional reports for, and
- Complementary User Entity Controls (CUECs) listed for the Asset Managers to evaluate whether those controls are in place and operating effectively in their organizations.

Understanding the scope and coverage of the report is a key step for the reviewers to be able to assess and address the risks that arise from the use of the service organizations. The scope of the report is the combination of the system being covered, the period coverage of the report (as of date (Type 1) or period of time (Type 2)), and the trust services categories that are included in the report. For Type 2 reports, the most common period coverage is 12 months, and Asset Managers should assess the operating effectiveness of controls if the coverage is less than 12 months.

The trust services categories themselves relate to areas of interest for the Asset Management firms. As described above, a SOC 2 could include one or more of the Trust Services Criteria, with common criteria being a baseline for all five categories and related criteria.

Because the criteria included within the report are determined by management of the service organization providing the report, it is important to ensure that the coverage is in line with the expectations of the Asset Management firm. To help better understand the categories and related criteria, included below are the definitions as defined by the AICPA:

- ***Security*** - Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.
- ***Availability*** - Information and systems are available for operation and use to meet the entity's objectives.
- ***Processing Integrity*** - System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.
- ***Confidentiality*** - Information designated as confidential is protected to meet the entity's objectives.
- ***Privacy*** - Personal information is collected, used, retained, disclosed, and disposed to meet the entity's objectives.

UNDERSTANDING THE NEW SOC FOR CYBERSECURITY REPORT

The AICPA has recently developed a SOC for Cybersecurity report, which assists organizations as they relay relevant and useful information about the effectiveness of their cybersecurity risk management program to management, directors, investors, business partners, and other stakeholders.

Although the SOC 2 engagement can provide users with insight into an organization's cybersecurity controls, there are many differences between the audience, subject matter, and scope of each service.

While a SOC 2 provides coverage of the system under AICPA's Trust Services Criteria, SOC for Cybersecurity can be entity-wide and use other suitable criteria such as NIST CSF or ISO 27001.

Asset Managers can obtain these reports to understand service organization's efforts on management of cybersecurity threats and whether effective processes and controls are in place to detect, respond to, mitigate and recover from breaches and other security events.

COMPARISON OF SOC REPORTS

The chart below provides a comparison of SOC reports available to Asset Managers for review and consideration.

	SOC 1	SOC 2	SOC 3	SOC for Cybersecurity
What is the subject matter of the report?	Controls at a service organization relevant to user entities internal control over financial reporting.	Controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy.	Controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy.	Controls relevant to an organization's enterprise-wide cybersecurity risk management program.
What is the purpose of the report?	To provide information to the auditor of a user entity's financial statements about controls at a service organization that may be relevant to a user entity's internal control over financial reporting. It enables the user auditor to perform risk assessment procedures, and if a type 2 report is provided, to assess the risk of material misstatement of financial statement assertions affected by the service organization's processing.	To provide management of a service organization, user entities, and other specified parties with information and a CPA's opinion about controls at the service organization that may affect user entities' security, availability, processing integrity, confidentiality or privacy.	To provide users with information about controls at the service organization that may affect user entities' security, availability, processing integrity, confidentiality or privacy.	To provide general users with information about the cybersecurity risk management program.
Who are the intended users?	Auditors of the user entity's financial statements, management of the user entities, and management of the service organization.	Parties that are knowledgeable about: • the nature of the service provided by the service organization • how the service organization's system interacts with user entities, subservice organizations, and other parties • internal control and its limitations • the criteria and how controls address those criteria.	General use reports, SOC 3 reports can be freely distributed.	Entity management, directors, investors, business partners, and other stakeholders.

SOC KEY TERMS

Service organization	An organization or segment of an organization that provides services to user entities, which are likely to be relevant to those user entities' controls over its system relevant to security, availability, processing integrity, confidentiality, or privacy.
Service auditor	A practitioner who reports on controls of a service organization's system, relevant to security, availability, processing integrity, confidentiality, or privacy.
User entity	An entity that uses a service organization. This entity may be a user of the services provided by the service organization. Constituents of the user entity include management such as those within finance, internal audit, compliance, and/or IT.
Subservice organization	A service organization used by another service organization to perform some of the services provided to user entities that are relevant to those user entities' security, availability, processing integrity, confidentiality, and/or privacy.
Inclusive method	Method of reporting that allows the description of controls to include controls in place at the subservice organizations.
Carve-out method	Method of reporting that does not allow the description of controls to include controls in place at the subservice organizations.

WWW.SIFMA.ORG