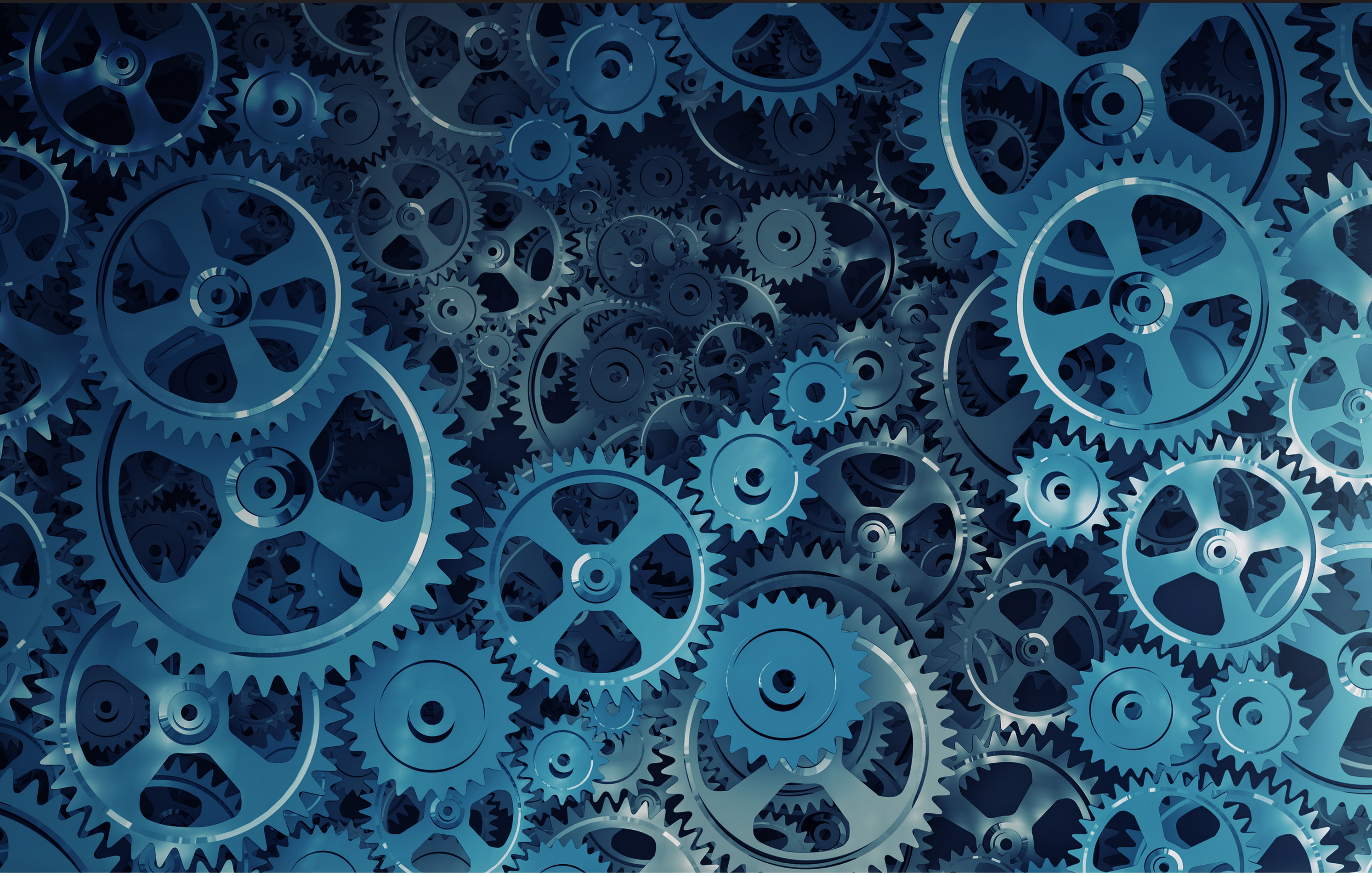
sifma

ASSET MANAGEMENT GROUP



ASSET MANAGER'S GUIDE TO SOC 1

JUNE 2017

At Grant Thornton, we help dynamic organizations navigate the complexities of today's business landscape, ensuring that our clients can respond to ever-changing regulations and investor demands. We go beyond the traditional compliance and reporting aspects of audit and tax, providing services that offer real value. In addition, our advisory services professionals are progressive thinkers who create, protect and transform value today so our clients have the opportunity to thrive tomorrow. Visit grantthornton.com for more information.

SIFMA Asset Management Group ("AMG") brings the asset management community together to provide views on policy matters and to create industry best practices. SIFMA AMG's members represent U.S. and multinational asset management firms whose combined global assets under management exceed $39 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.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Asset Management Group (AMG) of the Securities Industry and Financial Markets Association (SIFMA) has updated the Asset Manager's System and Organization Controls (SOC) 1 reports guide as a result of the American Institute of Certified Public Accountants' (AICPA) Clarity Project.

This *Asset Manager's Guide to SOC 1* reports was developed by Grant Thornton LLP, applying the *Asset Manager Guide to SAS 70* (issued in October of 2007, and available at http://www.sifma.org/ uploadedfiles/newsroom/ press_releases/assetmanagerguidesas-70.pdf), *Statement on Standards for Attestation Engagements (SSAE) No. 18, Attestation Standards: Clarification and Recodification* (effective as of May 1, 2017), and AICPA's *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting (SOC 1(R)) guide* (updated as of January 1, 2017).

The current updates are meant to provide the following:

- Background of the AICPA's Attestation Clarity Project
- Changes to the SSAE No. 18, Attestation Standards
- Changes from the AT-C sections impacting SOC 1 reports

The recommended asset manager baseline areas of scope and control objectives within this guide include asset management operations and Information Technology (IT) general computer controls. The baseline areas were developed to improve the quality and consistency of reporting for the industry. This document is meant to serve as a guide for defining the scope of a SOC 1, and is not a substitute for the guidelines defined in the AICPA's attestation standards and reporting guides.

HISTORY OF REPORTING ON INTERNAL CONTROLS OVER FINANCIAL REPORTING

SAS 70 was originally issued by AICPA in April 1992, with the goal of providing a detailed guide for an audit of the controls at a service organization related to financial statement reporting risks of user entities. The requirements and guidance for both service auditors reporting on controls at a service organization and user auditors auditing the financial statements of a user entity were contained in AU Section 324.

In 2010, the Auditing Standards Board issued SSAE 16, *Reporting on Controls at a Service Organization,* which was codified in the attestation standard (AT) 801. SSAE 16 included the requirements and guidance for service auditors only. The requirements and guidance for user auditors remained in AU Section 324.

In May 2011, the following AICPA guide was issued: Service Organizations: *Applying SSAE 16, Reporting on Controls at a Service Organization* (SOC 1) but was not conformed to the clarified auditing standard. In addition, in May 2013, the following AICPA guide was issued: *Service Organizations: Reporting on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting*.

In April of 2016, the AICPA's Auditing Standards Board (ASB) completed a Clarification Project on Statements on Standards for Attestation Engagements (SSAEs or attestation standards) and issued its clarified attestation standards as SSAE No. 18, *Attestation Standards: Clarification and Recodification.* SSAE No. 18 is effective for practitioners' reports dated on or after May 1, 2017.

In addition, in January of 2017, the following AICPA guide was updated to reflect the updates for SSAE No. 18: *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting (SOC 1(R)).*

Subsequently, the AICPA announced updated branding for System and Organization Controls reports, a suite of service offerings CPAs may provide in connection with system-level controls of a service organization or entity-level controls of other organizations, including the SOC 1® - SOC for Service Organizations: ICFR.

The attestation standards are developed and issued in the form of SSAEs and are codified into sections. The identifier "AT-C" is used to differentiate the sections of the clarified attestation standards from the sections of the attestation standards which are superseded by SSAE No. 18 as follows:

AT-C Sec. 105 – Concepts Common to All Attestation Engagements

AT-C Sec. 205 – Examination engagements

AT-C Sec. 210 – Review engagements

AT-C Sec. 215 – Agreed upon Procedures engagements

AT-C Sec. 305 – Prospective Financial Information

AT-C Sec. 310 – Reporting on Pro Forma Financial Information

AT-C Sec. 315 – Compliance Attestation

AT-C Sec. 320 – Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting

SOC 1® reports are now issued under AT-C sections 105, 205 and 320.

OVERVIEW AND CURRENT LANDSCAPE

SOC 1 reports help firms demonstrate that they have appropriate internal controls over financial reporting and are typically requested by the customers of asset managers. SOC 1 reports are primarily intended to be auditor-to-auditor communications.

In addition, asset managers utilize SOC 1 reports to meet client requests; help support numerous regulatory requirements; and when acting as fiduciaries for their clients, demonstrate that they have sound financial controls and safeguards, particularly around areas of operations and IT. The following should be considered by asset managers in connection with SOC 1 examinations and reports:

- Sarbanes-Oxley legislation does not mandate the issuance of the SOC 1 report; however, Sections 302 and 404, in particular, have increased the awareness and scrutiny of the design and operating effectiveness of internal controls.
- Recent industry and regulatory events are requiring greater awareness over the control environment and controls in place to manage risk and adopt new compliance procedures (i.e., Title IV of the Dodd-Frank Wall Street Reform and Consumer Protection Act).
- Increased scrutiny due to the regulatory environment, such as SEC's amendments to the custody and recordkeeping Rule 206(4)-2 under the Investment Advisors Act of 1940.
- An increasing number of organizations are outsourcing key components of their operations such as the IT, fund accounting, and custodian functions.
- Increased expectations of asset managers to have a SOC 1 examination and, in some cases, other reports based on various attestation standards (AT-C section 315, Compliance Attestation, etc.) and other operational due diligence requirements.

GLOBAL TRENDS

As organizations expand where they do business and with whom, the need to obtain assurance over controls has become a global issue. The International Accounting and Auditing Standards Board developed a global standard for service organizations, *International Standard on Assurance Engagements (ISAE) 3402.* ISAE 3402 can often be issued with minimal effort if a SOC 1 is already being performed.

If the service organization and user organization are domiciled in the **same country**, then consider using the **local standard**. If the service organization and/or the user organization are domiciled in **different countries,** then consider using international standards. The service organization should consult with their user organizations to determine what standards will be appropriate.

CHANGES FROM THE AT-C SECTIONS IMPACTING SOC 1 REPORTS

The following list includes revised standards which affect asset managers (service organizations) providing SOC 1 reports to their customers, as well as the service auditors that issue those reports.

- Enhanced service auditor's requirements have been included to evaluate evidence around completeness and accuracy of information provided by the service organization.
  - Management of the service organization is required to provide the service auditor with an understanding of how relevant information (e.g., populations, reports, etc.) is gathered or produced and provide additional documentation (e.g., reporting parameters, system queries, etc.) to the service auditor for evaluation of completeness, accuracy and sufficiency of evidence.
- The service auditor has additional requirements to assess whether controls identified by management of the service organization are suitably designed to achieve the control objectives.
  - Management of the service organization was already responsible for this, however, the service auditor will now review management's written risk assessment, and revisit risk assessment activities, to ensure that relevant risks that threaten the achievement of the control objective(s) are sufficiently considered in management's description.
- The service auditor relying on Internal Audit of the service organization must revisit the competence and objectivity of the Internal Audit function based on the revised definition.
  - Management of the service organization needs to provide the service auditor with a written acknowledgement that internal auditors providing direct assistance to the service auditor will be allowed to follow the service auditor's instructions, and that the service organization will not intervene in the work the internal auditors perform for the service auditor.
- The service auditor is required to review Internal Audit reports and regulatory examinations relating to the services provided to user entities and consider the findings in determining the nature, timing and extent of the tests to be performed in the SOC 1 report.
  - Management of the service organization should make the reports available to the service auditor and should also ensure that relevant issues identified in such reports are addressed timely.
- The service auditor must determine that the service organization's management assertion addresses all of the criteria used to evaluate the fairness of the presentation of the description, the suitability of the design of the controls, and the operating effectiveness of the controls (for Type 2).

  - Management of the service organization should identify and include all required criteria in the management assertion. If certain criteria are not applicable, they still need to be included in the assertion and in such cases management may want to explain why the criteria is not applicable in the management's description.
- When using the inclusive and carve-out methods of presentation for the subservice organizations in the SOC 1 report, additional requirements have been included for management of the service organization.
  - When using the carve-out method, management should identify complementary subservice organization controls (CSOCs). The standard defines CSOCs as 'controls that management of the service organization assumes, in the design of the service organization's system, will be implemented by the subservice organizations and are necessary to achieve the control objectives stated in management's description of the service organization's system'.
  - When using the carve-out method, management should evaluate and rationalize the existing list of subservice organizations in the report to identify the impacted control objectives, identify the broad types of controls that are expected at each subservice organization and link to the relevant control objective(s) that are impacted.
  - When using the inclusive method, management should assess their monitoring controls of the subservice organizations, and continue to include a description of such monitoring controls in management's description.
- Additional requirements have been included for management of the service organization to identify and remove controls stated in management's description that are not necessary to achieve the control objective(s).
  - Management of the service organization has to assess the description of the system and ensure that all controls that are necessary to achieve the control objectives are included and remove controls that are not necessary to achieve the control objectives.

SERVICE ORGANIZATION RESPONSIBILITIES

PRIMARY RESPONSIBILITIES:

- Confirming that the SOC 1 standard is appropriate to the financial reporting risks of user entities
- Defining the scope of the engagement (e.g., services, functional areas, application systems)
- Determining the type of engagement to be performed (Type 1 or Type 2)
- Determining the "as of date" for a Type 1 or the period to be covered by the report for a Type 2
- Determining whether services provided to a service organization by other entities are likely to be relevant to user entities' internal control over financial reporting, and if so, identifying these other entities as subservice organizations
- Determining whether subservice organizations will be included (inclusive method) or excluded (carve-out method) from the description of the service organization's system
- Selecting the criteria to be used, stating them in the assertion, and determining that the criteria are appropriate for management's purposes
- Preparing a description of the service organization's system, including the completeness, accuracy, and method of presentation of the description
- Specifying the control objectives; stating them in the description of the service organization's system; and if the control objectives are specified by law, regulation, or another party (for example, a user group or a professional body), identifying in the description the party specifying the control objectives
- Identifying the risks that threaten the achievement of the control objectives stated in the description of the service organization's system and designing, implementing, and documenting controls that are suitably designed and operating effectively to provide reasonable assurance that the control objectives stated in the description will be achieved
- Preparing a written assertion, that accompanies management's description of the service organization's system, both of which will be provided to user entities
- Having a reasonable basis for management's assertion
- Providing the service auditor with written representations at the conclusion of the engagement (When the inclusive method is used, management of the service organization and management of the subservice organization agree to provide and do provide such representations)
- If the service auditor plans to use internal auditors to provide direct assistance, providing the service auditor with written acknowledgement that internal auditors providing direct assistance to the service auditor will be allowed to follow the service auditor's instructions, and that the service organization will not intervene in the work the internal auditors perform for the service auditor
- Providing the service auditor with access to all information, such as records, documentation, service level agreements, and internal audit or other reports, that management is aware of and that are relevant to the description of the service organization's system and management's assertion
- Providing the service auditor with unrestricted access to personnel within the service organization from whom the service auditor determines it is necessary to obtain evidence relevant to the service auditor's engagement

- Disclosing to the service auditor the following:
  - Incidents of noncompliance with laws and regulations, fraud, or uncorrected errors attributable to management or other service organization personnel that are clearly not trivial and that may affect one or more user entities and whether such incidents have been communicated appropriately to affected user entities
  - Knowledge of any actual, suspected, or alleged intentional acts by management or the service organization's employees that could adversely affect the fairness of the presentation of management's description of the service organization's system or the completeness or achievement of the control objectives stated in the description
  - Any deficiencies in the design of controls of which management is aware
  - All instances in which controls have not operated as described
  - Any events subsequent to the period covered by management's description of the service organization's system, up to the date of the service auditor's report, that could have a significant effect on management's assertion

SECONDARY RESPONSIBILITIES:

- Identify project coordinator and key contacts
- Assist the service auditor in determining logistical requirements for testing such as access to system(s), reports and documentation
- Reviewing and editing the final draft of the SOC 1 report
- Controlling the distribution of the SOC 1 report

SERVICE AUDITOR RESPONSIBILITIES

PRIMARY RESPONSIBILITIES:

- Determining whether to accept or continue an engagement for a particular client
- Establishing an understanding with management of the service organization regarding the services to be performed and the responsibilities of management and the service auditor, which ordinarily is documented in an engagement letter
- Assessing the suitability and availability of the criteria management has used in preparing the description
- Obtaining an understanding of the service organization's system
- Assessing the risk of material misstatement
- Requesting a written assertion about whether the subject matter is in accordance with or based on the criteria
- Responding to assessed risk and obtaining evidence
- Evaluating whether management's description of the service organization's system is fairly presented
- Evaluating whether control objectives are reasonable and relevant to user' entities' internal controls over financial reporting
- Obtaining and evaluating evidence regarding the suitability of the design of the controls

- Obtaining and evaluating evidence regarding the operating effectiveness of controls in a Type 2 engagement
- Determining which controls to test
- Designing and performing tests of controls
- Using the work of the internal audit function, if applicable
- Evaluating the results of procedures
- Describing tests of controls and the results of tests
- Linking controls to risks
- Performing procedures to address complementary user entity controls and complementary subservice organization controls
- Forming the opinion and disclaiming an opinion on "other information" provided by the service organization, if applicable
- Performing procedures to address any instances of fraud, illegal acts or uncorrected errors; design deficiencies in controls; test operating effectiveness deficiencies; and subsequent events in which management makes the service auditor aware that would have a significant effect on a user organization
- Reading the reports of internal audit reports function and regulatory examinations that relate to the services provided to user entities and the scope of the engagement
- Preparing the Service Auditor's Report (the opinion)
- Obtaining written representations

SECONDARY RESPONSIBILITIES:

- Meet with service organization to finalize scope, specific objectives to be accomplished by examination, and responsibilities, and schedule field work
- Finalize engagement work plan and schedule staff
- Discuss findings and recommendations with the service organization

FORM AND CONTENT OF SOC 1 TYPE 1 AND TYPE 2 REPORTS

There is no **rigid standard** proposed by AICPA guidance with regards to the organization of a SOC 1 report; however, leading practices indicate that the report should be organized as follows:

Section 1 Independent Service Auditor's Report (the opinion).

Section 2 Management's assertion and, if applicable, a subservice organization's management assertion.

Section 3 Management's description of the service organization's system.

Section 4 Management's control objectives and control activities. Type 2 reports also include the independent service auditor's tests of controls and results of tests.

Section 5 Other information provided by the service organization. This is an optional section and the service auditor does not opine on such information. Content typically includes information related to the service organization's disaster recovery plan, compliance with other regulatory standards or management responses to testing exceptions.

SOC 1 Type 1	SOC 1 Type 2
Reports on controls placed in operation	Reports on controls placed in operation and tests of operating effectiveness
• Report is as of a point in time (e.g., as of 12/31/201X) • Opinion rendered related to the fair presentation of the description • Opinion rendered related to the suitability of the design of the controls • No opinion rendered related to the operating effectiveness of the controls • Not considered useful for purposes of reliance by user auditors • Not used as a basis for reducing the assessment of the control risk below the maximum • Generally performed for the first year a service organization pursues a SOC 1 report	• Report covers a period of time, generally between six and 12 months • Opinion rendered related to the fair presentation of the description • Opinion rendered related to the suitability of the design of the controls • Opinion rendered related to the operating effectiveness of the controls • May provide user auditors with a basis for reducing assessment of control risk below the maximum • Requires more internal and external effort • Identifies instances of noncompliance of the stated control activity

For additional guidance regarding the Independent Service Auditor Reports for Type 1 and Type 2 reports, see the following:

Reporting on Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting guide (2017) – Chapter 2

DEFINING THE DESCRIPTION OF CONTROLS

The service auditor can assist in writing the description of controls; however, the **service organization must take responsibility** for the completeness, accuracy and method of presentation. The description should provide information about the service organization's internal control that is **relevant** to the user organization's internal control over financial reporting.

At a minimum, the description of controls should include the following:

- Aspects of the service organization's **control environment, risk assessment, information and communication, and monitoring** that may affect the services provided to the user organization as it relates to an audit of financial statements
- Control objectives, related controls, and user control considerations pertaining to operations and **general computer controls**
- Changes to the controls since the later of the date of the last report or within the last 12 months

ASSET MANAGER SCOPE

Areas relevant to an asset manager are categorized as one of the following as it relates to the scope of an asset manager SOC 1:

Baseline: This area is relevant to a user organization's internal control as it relates to internal controls over financial reporting and is common to the scope of SOC 1 issued by asset managers.

Not Baseline: This area is not relevant to a user organization's internal control as it relates to internal controls over financial reporting and is not common to the scope of SOC 1 issued by asset managers.

Other Areas to Consider: This area is not common to the scope of SOC 1 issued by asset managers, but may be considered for inclusion in scope.

"Baseline" areas, "Not Baseline" areas, and "Other Areas to Consider" for an asset manager's SOC 1 report are depicted on the following pages as it relates to:

- Control environment
- Operations
- General computer controls

ASSET MANAGER SCOPE: CONTROL ENVIRONMENT

Baseline	Not Baseline
• Integrity and ethical values • Commitment to competence • Board of directors or audit committee participation • Management philosophy and operating style • Organizational structure • Assignment of authority and responsibility • HR policies and procedures • Risk assessment • Information and communication • Monitoring	Privacy policies and procedures In general: • The Control Environment is the foundation for all other aspects of internal control and, therefore, it is essential that the service organization describe the appropriate information in the description of controls based on what is relevant to the user organizations. • The service auditor is also responsible for evaluating/testing the information included in the control environment description. • Management is not precluded from presenting relevant aspects of its control environment in the form of a control objective with applicable controls listed.

ASSET MANAGER SCOPE: OPERATIONS

Baseline	Not Baseline/Other Areas to Consider
• New Account Setup and Account Maintenance • New Security Setup and Maintenance • Contributions / Distributions • Trading - Trade Processing - Client Investment Guideline and Restriction Compliance - Trade Allocation - Trade Error and Investment Guideline Breaches - Trade Settlement Procedures • Investment Income • Valuation (Securities, Foreign Exchange Rates and Derivatives) • Corporate Actions • Reconciliation (Cash and Position) • Client Reporting	**Not Baseline** • Investment Adviser Registration, Form ADV, and Delivery Requirements Policies and Procedures • Section 13 filings under the Securities Exchange Act of 1934 Policies and Procedures • Advertising and Marketing Investment Services • Insider Trading • Portfolio Pumping and Window Dressing • Client Complaint Processing • Product Development • Cross Trading • Managing Proprietary Accounts • Cash Referral Fee Agreement • Account Performance • Laws and Regulations • Irs Rules **Other Areas to Consider** • Fee Calculation and Billing • Custody or Possession of Client Assets (Depends on if Applicable) • Brokerage Allocation (Includes Best Execution, Affiliated Trading, Soft Dollars, Directed Brokerage and IPO or New Issues Allocation) • Broker Selection and Retention • Trading Aggregation • Proxy Voting • Personal Trading • AML Review

ASSET MANAGER SCOPE: GENERAL COMPUTER CONTROLS

Baseline	Not Baseline
• Information Systems Operations - Job scheduling - Record backup - Incident management • Information Security - Logical security - Physical security - Environmental protection • Change Management - Application changes - System software changes - Network changes - Hardware changes	Business Continuity Planning or Disaster Recovery* * Note: In accordance with AICPA guidance, a service auditor cannot form an opinion on the design of controls or operating effectiveness over business continuity planning or disaster recovery.

DETERMINING THE CONTROL OBJECTIVES

- The control objectives should be determined by the service organization, taking into consideration the needs of the service organization's users and their independent auditors relating to internal controls over financial reporting. However, the service auditor may assist the service organization with defining appropriate control objectives in the following ways:
  - By providing examples of control objectives that may be relevant to user organizations as it relates to internal controls over financial reporting
  - By reviewing draft control objectives and providing feedback as to their appropriateness and adequacy
- The control objectives may be designated by the service organization or outside parties such as regulatory authorities, a user group or others.
- If the control objectives are incomplete, the service auditor may qualify the SOC 1 report.
- Control objectives help the user auditor determine how the service organization's controls affect the user organization's financial statement assertions (i.e., validity, completeness, cutoff, recording, valuation and presentation).
- The service organization should establish control objectives that it believes relate to its users' financial statement assertions and provide a framework for the user auditors to assess control risk as a whole.
- The service organization can modify control objectives after the start of the engagement (may need to disclose this in the report in an explanatory paragraph). However, the service organization cannot modify a control objective to "get out" of a control objective, which would be considered significant by user organizations and their auditors, or if there is a significant deficiency in either the design or operating effectiveness of the controls.

BASELINE CONTROL OBJECTIVES

Area	Baseline Control Objectives
New Account Setup and Maintenance	Controls provide reasonable assurance that documentation for the opening and modification of client accounts is received, authenticated, and established accurately, completely, and in a timely manner on the applicable system.
Trading/Settlement • Allocation • Processing • Settlement	Controls provide reasonable assurance that trades are properly authorized, settled, and recorded in accordance with portfolio guidelines and relevant account restrictions, accurately, completely, and in a timely manner in the client account.
	Controls provide reasonable assurance that block orders are allocated to client accounts according to management established methodologies, and allocations are approved by management.
Contributions/Distributions	Controls provide reasonable assurance that contributions and distributions are authorized by the client and processed and recorded accurately, completely, and in a timely manner in the client account.
New Security Setup and Maintenance	Controls provide reasonable assurance that new securities and changes to existing securities are authorized and processed accurately, completely, and in a timely manner.
Valuation (Securities, Foreign Exchange Rates, and Derivatives)	Controls provide reasonable assurance that valuation, including securities, foreign exchange rates, and derivatives, is received from an authorized source and updated accurately, completely, and in a timely manner.
Investment Income	Controls provide reasonable assurance that interest and dividend income information is received from an authorized source and processed accurately, completely, and in a timely manner in the client account.
Corporate Actions	Controls provide reasonable assurance that corporate actions are received from an authorized source and processed accurately, completely, and in a timely manner in the client account.
Reconciliation	Controls provide reasonable assurance that cash and security positions reflected in the portfolio accounting system reconcile to actual positions and balances held by custodians, and discrepancies are identified, researched, and resolved in a timely manner.
Client Reporting	Controls provide reasonable assurance that account statements reflect the correct holdings and market value and are provided to clients in a complete and timely manner.

Area	Baseline Control Objectives
Information System Operations	Controls provide reasonable assurance that production programs needed to process batch and online transactions are valid and executed and monitored timely and to normal completion.
	Controls provide reasonable assurance that data is backed up, retained and retrievable.
	Controls provide reasonable assurance that processing incidents are identified, tracked, recorded, and resolved accurately, completely, and in a timely manner.
Information System Security	Controls provide reasonable assurance that logical security tools and techniques are configured, administered, and monitored to enable restriction of access to programs, data, and other information resources.
	Controls provide reasonable assurance that physical access restrictions are implemented and administered to ensure that only authorized individuals have ability to access or use information resources.
	Controls provide reasonable assurance that information resources are protected against environmental hazards and related damage.
Information System Change Management	Modifications and upgrades to applications, the network, hardware, and systems software are authorized, approved by management, tested, and implemented accurately, completely, and in a timely manner.

ELEMENTS OF CONTROL OBJECTIVES

The table below presents the categories of assertions that may exist in a user entities' financial statements and that may be affected when the service provided by the service organization involves processing transactions and recording events for user entities. For additional guidance regarding the user entities' financial statement assertions, see the following:

Reporting on Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting guide (2017) – Chapter 4

User Entities' Financial Statement Assertions	Illustrative Examples of Service Organization's Control Objectives	Illustrative Examples of Risks That Threaten the Achievement of the Control Objectives as They Relate to the User Entities' Financial Statements
Occurrence. Transactions and events that have been recorded have occurred and pertain to the entity.	Controls provide reasonable assurance that transactions are authorized and received only from authorized sources. Controls provide reasonable assurance that transactions are validated in a complete, accurate, and timely manner.	Unauthorized transactions are entered and not detected. For example, manual transactions are not reviewed and approved by authorized individuals, or transactions are entered by unauthorized individuals. Invalid transactions are entered and not detected. For example, duplicate transactions are entered. Entered transactions are not validated against master data and other management authorization criteria. For example, automated transactions are not validated against master data, or transactions that do not correspond with master data are not rejected. Transactions are incorrectly processed so that invalid transactions are recorded, for example, recorded as a result of a logic error in the application. Transaction reports provided to user entities inappropriately accumulate transactions. For example, transaction reports include invalid transactions or information that is inconsistent with the transaction detail maintained by the service organization.

User Entities' Financial Statement Assertions	Illustrative Examples of Service Organization's Control Objectives	Illustrative Examples of Risks That Threaten the Achievement of the Control Objectives as They Relate to the User Entities' Financial Statements
Completeness. All transactions and events that should have been recorded have been recorded.	Controls provide reasonable assurance that transactions are entered, processed, recorded, and reported in a complete manner.	All authorized and valid transactions are not recorded. For example, transactions are incorrectly rejected, are not properly reentered, are not entered on a timely basis, or are recorded in the accounts of the wrong entity. Applications incorrectly process transactions so that all authorized and valid transactions are not recorded. For example, all transactions are not processed, processing is incomplete, or programming logic is incorrect Transaction reports provided to user entities inappropriately accumulate valid and authorized transactions. For example, valid transactions are excluded, or reported information is inconsistent with transaction detail maintained by the service organization.

User Entities' Financial Statement Assertions	Illustrative Examples of Service Organization's Control Objectives	Illustrative Examples of Risks That Threaten the Achievement of the Control Objectives as They Relate to the User Entities' Financial Statements
Accuracy. Amounts and other data relating to recorded transactions and events have been recorded appropriately.	Controls provide reasonable assurance that transactions are entered, processed, recorded, and reported in an accurate manner.	Inaccurate or incomplete amounts or other relevant transaction data are entered and not detected. For example, expected transaction data is missing, does not match expected field values, or does not fall within predetermined limits. Applications process transactions incorrectly, so that transactions contain inaccurate amounts or inaccuracies in other relevant transaction data. For example, a logic error in the application results in incorrect programmed calculations. Transaction reports provided to user entities inappropriately accumulate transactions. For example, reports include transactions containing inaccurate amounts or inaccuracies in other relevant data. Inaccurate or incomplete amounts or other relevant data are recorded or reported as a result of compromises in IT general controls.

User Entities' Financial Statement Assertions	Illustrative Examples of Service Organization's Control Objectives	Illustrative Examples of Risks That Threaten the Achievement of the Control Objectives as They Relate to the User Entities' Financial Statements
Cutoff. Transactions and events have been recorded in the correct accounting period.	Controls provide reasonable assurance that transactions are entered, processed, recorded, and reported in a timely manner.	The incorrect period is entered for the transaction or the period is omitted and is not detected. Applications process transactions incorrectly so that transactions are recorded or reported in an incorrect period, for example, as a result of a logic error in the application. Transactions are recorded or reported in the wrong period as a result of compromises in IT general controls. Entered transactions are not validated in a timely manner.
Classification. Transactions and events have been recorded in the proper accounts.	Controls provide reasonable assurance that transactions are recorded and reported in the proper accounts.	An incorrect account is entered for a transaction and is not detected. Applications process transactions incorrectly, so that transactions are recorded in the wrong account, for example, as a result of a logic error in the application. Transaction reports provided to user entities inappropriately accumulate transactions, resulting in transactions being reported in the wrong accounts. Transactions are classified in the wrong accounts as a result of compromises in IT general controls.

SOC 1 KEY TERMS

User Organization	The entity that has engaged a service organization and whose financial statements are being audited.
User Auditor	The auditor who reports on the financial statements of the user organization.
Service Organization	The entity (or segment of an entity) that provides services to the user organization that is part of the user organization's information system.
Service Auditor	The auditor who reports on controls of a service organization that may be relevant to a user organization's internal control as it relates to an audit of financial statements.
Subservice Organization	An entity that performs functions or processing for the service organization that may be part of the user organization's information system as it relates to an audit of financial statements.
Inclusive Method of Reporting	Method of reporting that allows the description of controls to include controls in place at the subservice organizations.
Carve-out Method of Reporting	Method of reporting that does not allow the description of controls to include controls in place at the subservice organizations.

SOC 1 GUIDANCE RESOURCES

AICPA LITERATURE — AUDIT AND ACCOUNTING GUIDES:

Service organizations applying SSAE No. 18

- Based on the professional standards for performing a SOC 1 (AT-C sections 105, 205 and 320)
- Prepared by the AICPA SOC Task Force
- Useful when preparing and/or utilizing a SOC 1 report
- Provides guidance in applying generally accepted auditing standards in audits of financial statements of entities that use service organizations and in service auditors' engagements
- Information provided could be used to help determine the relevant business activities/control objectives to include in SOC 1

Industry guides:

- Various industry guides published by AICPA, including employee benefits, investment companies, and brokers and dealers

WWW.SIFMA.ORG