INVESTMENT COMPANY INSTITUTE®

ICI OPERATIONS

AUGUST 2020

Financial Intermediary Controls and Compliance Assessment Engagements

Financial Intermediary Controls and Compliance Assessment Engagements

Contents

Financial Intermediary Controls and Compliance Assessment Engagements

I. Introduction

The mutual fund industry continues to rely heavily on financial intermediaries, such as broker-dealers, to sell (distribute) mutual fund shares and provide services to end investors. Financial intermediary relationships are often complex arrangements and require oversight by management of the fund. As mutual fund distribution through intermediaries has evolved, many intermediaries have moved away from supporting individual shareholder accounts at the fund that are under broker control in favor of holding aggregated "omnibus" accounts with the fund representing shares that are beneficially owned by multiple shareholders.

Omnibus accounts hold mutual fund shares that are registered with the mutual fund's transfer agent in the name of the financial intermediary. The intermediary maintains the underlying shareholder account information on its own recordkeeping systems—a process known as subaccounting—and reports share transactions to the funds on an aggregate basis. The intermediary or its agent handles all communications and servicing of its customer accounts. As a result, the underlying shareholders in an omnibus account do not directly interact with the fund organization, and the mutual fund organization may have limited to no knowledge or transparency about the underlying shareholders.

As regulatory initiatives continue to create new or expanded regulatory compliance requirements, mutual fund complexes are challenging, and continuing to enhance, their oversight procedures to ensure that financial intermediaries are meeting their obligations.

Intermediary Oversight

Given the financial intermediary's direct control over and knowledge of its customers' fund positions, mutual fund oversight often includes monitoring certain intermediary activities to ensure adherence to mutual fund regulations, contractual obligations, and compliance with the terms of mutual fund prospectuses and statements of additional information (SAIs). Many mutual fund complexes have implemented policies and procedures that enable them to obtain information about the effectiveness of an intermediary's compliance controls, which may include on-site examinations, certifications, receipt of transparency data, review of analytics, and questionnaires. However, some of these methods may be duplicative and inefficient for intermediaries that have agreements with multiple fund complexes.

Increased Efficiency and Transparency

Recognizing the benefits of creating a standardized and efficient way for financial intermediaries to provide information about the effectiveness of controls related to key operational areas, a 2008 working group of Investment Company Institute (ICI) member firms and representatives of the national accounting firms developed the Financial Intermediary Controls and Compliance Assessment (FICCA) framework. The framework provides criteria for assessing controls at intermediaries to address key areas for which mutual fund complexes typically seek assurance. In addition, the framework includes additional information on the intermediary's key policies and procedures as well as certain controls that are not subject to controls testing.

Independent Assessment

The FICCA framework calls for the financial intermediary, as omnibus account recordkeeper, to engage an independent accounting firm to assess its internal controls (also referred to as, simply, *controls*) over specified activities that the intermediary performs for its shareholder accounts. This engagement is performed by a CPA (known as a *practitioner* or *service auditor*) under attestation standards established by the American Institute of Certified Public Accountants (AICPA). The practitioner performs an examination engagement for the financial intermediary (known as the *service organization*) to determine whether the intermediary's controls over the specified activities were suitably designed and operating effectively to achieve the related control objectives. Management of the financial intermediary provides the practitioner with a written statement (known as an *assertion*) about whether the intermediary's controls were suitably designed and operating effectively to achieve the control objectives. Consistent with current attestation standards and the type of examination engagement, the practitioner will express an opinion either on whether management's assertion is fairly stated in all material respects[1] or directly on the intermediary's controls. An illustrative practitioner's report and management assertion for this type of engagement are provided in Section V. Mutual fund complexes (known as *user entities*) may use the service auditor's report as one data point in their intermediary oversight program.

Additional Intermediary Information

Beyond the practitioner's engagement, the FICCA framework also directs intermediaries to provide additional critical information and context about key policies and procedures (known as *additional intermediary information*) related to their business environment. In some instances, controls related to additional information may also be presented, but testing would not be required. Although the additional intermediary information is not covered by the service auditor's report and management's assertion, this information is no less important in obtaining a comprehensive understanding of the financial intermediary's business environment. The additional intermediary information may or may not be incorporated in the same physical document or electronic file as the practitioner's report and management's assertion; the section containing the additional intermediary information will be clearly identifiable as "other information," and the service auditor's report generally will indicate that the other information is not covered by the service auditor's report.[2]

Flexible, Efficient Framework

The FICCA framework developed by the fund industry identifies 17 areas of focus for which mutual fund complexes typically seek assurance.

- Fourteen areas of focus address controls at the financial intermediary that may be assessed and tested by the service auditor as part of an examination attestation engagement.[3] The areas of focus that contain controls that are subject to testing by the practitioner are referred to as *control areas* in the remainder of this document. Examples of control areas include document retention and recordkeeping, transaction processing, shareholder communications, privacy protection, and anti–money laundering. The full list is presented in subsequent sections of the document (see page 6).

[1] AT-C Section 205, *Examination Engagements,* paragraph 79, states that in instances where one or more material misstatements based on the criteria result in a qualified opinion, the practitioner should express a qualified or adverse opinion directly on the subject matter even when the assertion acknowledges the misstatement.

[2] AT-C Section 205, *Examination Engagements*, states the following in paragraph 57, *Other Information*: "If prior to or after the release of the practitioner's report on AT-C Section 205, *Examination Engagements* subject matter or an assertion, the practitioner is willing to permit the inclusion of the report in a document that contains the subject matter or assertion and other information, the practitioner should read the other information to identify material inconsistencies, if any, with the subject matter, assertion, or the report. If on reading the other information, in the practitioner's professional judgment (Ref: par. .A67–.A68) (a) material inconsistency between that other information and the subject matter, assertion, or the report exists or (b) material misstatement of fact exists in the other information, the subject matter, assertion, or the report, the practitioner should discuss the matter with the responsible party and take further action as appropriate."

[3] This paper will collectively refer to examinations conducted under AT-C 205 and AT-C 320 as *examination attestation engagements*.

» Three additional areas of focus provide mutual fund complexes with critical information and context about the intermediary's business environment, including related policies and procedures. These areas of focus do not include controls that are tested by the practitioner, nor are they covered by management's assertion. To distinguish these three areas of focus from the control areas, and to be consistent with the reference to *other information* in AT-C 205, *Examination Engagements*, they will be referred to as *information areas* in the remainder of the document.

Additional details regarding all 17 areas of focus are provided in Sections II and III of the FICCA framework.

Independent Assessment Considerations

The financial intermediary determines the scope of the practitioner's examination of the 14 control areas, including identification of control areas relevant to the intermediary's business and the extent to which the practitioner will examine each control area. It is expected that all control areas within the FICCA framework will be addressed, unless a control area is not applicable to the intermediary. Numerous factors, such as the intermediary's use of third-party providers (known as *subservice organizations*) or the type(s) of control reporting to satisfy the FICCA framework, will cause the activities of each examination attestation engagement to vary, as described below. The specific terms of the engagement are agreed on by the practitioner and management of the financial intermediary.

From its inception, the FICCA framework has been based on the premise that intermediaries should have flexibility in providing fund complexes with independent assessments of the 14 control areas defined in the framework. For example, an examination attestation engagement may cover all 14 control areas through an engagement performed under AT-C 205, *Examination Engagements,* or through a combination of an examination report resulting from an engagement performed under AT-C 205 and other examination reports that address controls. For example, a system and organization controls (SOC) 1 report issued under AT-C 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting,* is specifically intended for use by management of the user entities (funds) and the user entities' auditors to evaluate the effect of the controls at the service organization on the user entities' internal control over financial reporting. If the financial intermediary has previously engaged a practitioner to perform an examination under AT-C 320 that covers certain aspects of its operations included in the FICCA framework, the AT-C 205 engagement and related report could be used to provide assurance on the control areas that are not covered by the practitioner's SOC 1 report.[4] This avoids the need for the practitioner to perform duplicate testing and reporting. As stated previously, it is up to the intermediary and the practitioner, when defining the examination attestation engagements covering the FICCA framework, to decide how FICCA-related testing and reporting to mutual fund complexes should occur.

Potential Intermediary Benefits

Recognizing the value of a practitioner's report on a financial intermediary's controls, many fund complexes have encouraged and requested such examination reports from their most significant financial intermediary relationships. In response to these requests, a growing number of financial intermediaries have undergone examination attestation engagements that address the FICCA control areas and have provided their practitioner's report on these engagements and supporting materials (e.g., policies and procedures addressing the three information areas of focus) to mutual fund personnel tasked with overseeing the financial intermediaries' activities. By doing so, the intermediaries may reduce or eliminate the need for overlapping compliance evaluations by each fund complex.

[4] If a multi-report strategy is employed to meet the FICCA framework, a control area should be fully covered in either the SOC 1 report or the examination report. If only part of a control area is covered in a SOC 1 report or other report, the full control area should be covered in the FICCA examination report.

Ongoing Evaluation of FICCA Framework

Since creating the FICCA framework, ICI has formed a standing working group of ICI member firms, national accounting firm members, and financial intermediaries to periodically review and, as necessary, update the FICCA framework. As the use of this oversight tool expands and matures, working group evaluations are intended to enhance the information provided by these reports and promote the broadest adoption by financial intermediaries and funds. The working group has several ongoing objectives:

- Provide a forum to share experiences and develop a better understanding of the scope of FICCA reports issued to date
- Validate that the FICCA areas of focus, including its control areas for which the practitioner performs test of controls, are still current and appropriate to ensure that intermediaries are meeting their compliance and contractual obligations
- Review and update the framework based on feedback provided
- Streamline and improve this document, where appropriate, to help practitioners, financial intermediaries, and fund complexes in planning and executing the attestation engagement and subsequently using FICCA engagement reports
- Ensure that this document remains consistent with current AICPA standards governing attestation engagements

Major revisions to the FICCA framework are summarized by date in Section VIII.

For More Information About the FICCA

Fund, intermediary, or audit firm representatives who are interested in learning more about the FICCA should contact Marty Burns, ICI chief industry operations officer, at mburns@ici.org or 202-326-5980; Jeff Naylor, ICI director of operations and distribution, at jeff.naylor@ici.org or 202-326-5844; or Greg Smith, ICI senior director of fund accounting and compliance, at smith@ici.org or 202-326-5851.

II. About the FICCA Framework

Overview and Objective

The Financial Intermediary Controls and Compliance Assessment (FICCA) framework document is intended to provide criteria and guidance to (1) financial intermediaries that engage independent accountants to assess and report on their controls over key mutual fund shareholder servicing and recordkeeping activities and (2) mutual fund complexes that use these reports as part of their ongoing due diligence programs.

Key terms used in the FICCA framework are defined as follows:

- **User entity:** The entity that uses the services of the financial intermediary (typically the fund complex).
- **Service organization:** The financial intermediary organization that initiated the FICCA engagement.
- **Subservice organization:** A service organization used by the financial intermediary to perform services that are likely to be relevant to the user entities and related to control areas in the FICCA framework. The subservice organization may provide a SOC 1 report that addresses control areas in the FICCA framework (e.g., subaccount billing, invoice processing).
- **Control objectives:** The aim or purpose of specified controls at a service organization (the financial intermediary). Management's control objectives are included in the intermediary's description of its system and in the section of a type 2 SOC 1[5] report that contains the service auditor's description of tests of controls and results. SOC 1 reports are issued under AT-C 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting,* of the attestation standards established by the AICPA. In a type 2 SOC 1 engagement, the service auditor is required to test the operating effectiveness of the controls intended to achieve the related control objectives. There are 14 control areas of focus defined as control objectives within the FICCA framework.

A more detailed glossary of terms used in the FICCA framework is provided in Section IV.

[5] A report issued under AT-C 320 is one of several examination control reports provided for in the AICPA's SOC series of reports. A type 2 SOC 1 report includes a description of the service auditor tests of the operating effectiveness of the controls and the results of those tests. A type 1 SOC 1 report does not include this description.

Areas of Focus

Each of the 17 areas of focus listed below and described in the FICCA framework should be addressed annually as part of the financial intermediary's examination attestation engagements.

The first three areas of focus (e.g., information areas) provide important background and context for the financial intermediary's business environment. Any controls included in the additional intermediary information are not assessed and tested by the practitioner, so they are not included as part of management's assertion or the independent auditor's reports.[6] Management provides documentation about these areas to the fund complex to describe the policies, procedures, and (if applicable) controls that are in place for these information areas of focus:

1. Management reporting (quality control)
2. Risk governance program
3. Third-party oversight

The remaining 14 areas of focus (e.g., control areas) have controls that are assessed and tested by a practitioner on an annual basis, and the results of the practitioner's tests should be provided to fund complexes through one of the financial intermediary's examination attestation reports (e.g., reports issued under AT-C 205 or AT-C 320):

4. Code of ethics
5. Information security program
6. Anti–money laundering (AML) and the prevention of terrorist financing program
7. Document retention and recordkeeping
8. Security master setup and maintenance
9. Transaction processing—financial and nonfinancial (e.g., account setup and maintenance)
10. Cash and share reconciliations
11. Lost and missing security holders
12. Shareholder communications
13. Subaccount billing, invoice processing
14. Fee calculations
15. Information technology (including internet and VRU)
16. Business continuity/disaster recovery program
17. State of sale reporting (for blue sky purposes)

[6] Refer to paragraph .57 of AT-C Section 205, *Examination Engagements*, which addresses *other information*.

Format

In Section III, the FICCA framework is presented in two tables organized by area of focus. The first table pertains to the three information areas of focus. Policies, procedures, and any controls presented in the information areas typically are not assessed and tested by the practitioner. The second table refers to the 14 control areas of focus, the controls of which are assessed by the practitioner for suitability and tested for effective operation. Column headings within the tables are defined as follows:

Table 1: Information Areas 1–3

Area of focus/information area: The area of focus to which additional intermediary information pertains.

Considerations for response: Points for financial intermediary consideration when providing documentation that describes the policies, procedures, and controls for the related area of focus. Responses should be tailored on the basis of the intermediary's actual operations. Points presented are neither a checklist nor a comprehensive listing of all relevant factors that may exist in each business environment.

Table 2: Control Areas 4–17

Area of focus/control area: The 14 areas of focus/control areas that are assessed and tested by the practitioner.

Potential reporting mechanism: Various report types available to financial intermediaries that may address the control area and results of any testing performed. Options include the following reports that pertain to the financial intermediary (service organization) or a third-party service provider (subservice organization):

- An examination report issued under AT-C 205[7]
- A SOC 1 report issued under AT-C 320 and the SOC 1 Guide[8]

Financial intermediaries must review their own report environment for applicability.[9]

Control objective: The aim or purpose of specified controls. The practitioner tests controls to determine whether the controls described are suitably designed and operating effectively to achieve the related control objective.

Considerations for response: Illustrative guidance to be considered by financial intermediaries when defining controls to achieve the control objectives.

---

[7] Reports that are issued under AT-C 205 *Examination Engagements* should address at least one of the control areas outlined in the FICCA framework, as agreed to by management of the financial intermediary and the practitioner conducting the engagement.

[8] SOC 1 reports issued under AT-C 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting,* clearly identify any information in a SOC 1 report that is not covered by the practitioner's report by placing that information in a separate section of the SOC 1 report and identifying that section as "other information."

[9] Although not typical, a SOC 2 report issued under AT-C 205 *Examination Engagements* and the AICPA guide, *SOC 2 Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* could address FICCA focus areas. The SOC 2 report would need to include the availability, confidentiality, security, and processing integrity trust services criteria categories as referenced in the AICPA publication *TSP Section 100: 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.* The FICCA framework would need to be explicitly included as one of the SOC 2 report's principal service commitments and system requirements; guidance about service commitments and system requirements is found in the AICPA publication *DC Section 200: Description Criteria for a Description of a Service Organization's System in a SOC 2 Report.*

III. FICCA Framework

Table 1: Information Areas of Focus 1–3

Information area	Considerations for response
1. Management reporting (quality control)	Describe the overall oversight program and escalation procedures that support the quality assurance process, including the general tools and processes that are used by management to ensure quality and allow management to monitor the organization.
2. Risk governance program	Describe the following: » overview of the service organization; » identification of key business processes; » management oversight and controls; » responsibilities for risk governance and internal control; » legal and compliance responsibilities; » information technology; » use of subservice organizations; and » other considerations for users of the report (e.g., control activities that should be present at user entities [referred to as *complementary user entity controls*]). Other considerations include a description of the service organization's: » risk assessment process; » documentation of the risk assessment process; and » senior management and/or board review and approval.
3. Third-party oversight	Describe your third-party oversight program, including: » whether the service organization uses subservice organizations that are relevant to FICCA areas of focus; » all subservice organizations that are relevant to FICCA areas of focus; » subservice organization location—on-site, off-site, offshore; » employee background checks; » compliance awareness training; » assessment process for subservice organizations' business continuity/disaster recovery plans; and » service organization's policy/practice related to using subservice organizations: » how long this has been a practice; » communication protocols; » conditions under which subservice organizations are used; » how subservice organizations are trained and held to the service organization's standards (e.g., privacy protection); and » whether the subservice organization has an AT-C 320 report or other form of external oversight report—if not, how the company gains comfort with the subservice organization's control environment. **NOTE:** When addressing the third-party oversight information area of focus, financial intermediaries may find helpful Trust Services Principles (TSP) Criterion CC9.2 in AICPA's publication, *TSP Section 100: 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* regarding risk management and assessment associated with vendors and business partners. Fund complexes are seeking a reasonable understanding of the intermediary's third-party oversight program applied to each subservice organization that is relevant to FICCA areas of focus. Information provided should address the financial intermediary's unique oversight program for each third party that performs distinct functions related to each FICCA area of focus. It is anticipated that financial intermediaries will disclose any significant situation where a subservice organization does not meet expected shareholder servicing standards.

Table 2: Control Areas of Focus 4–17

Control area	Potential reporting mechanism		Control objective	Consideration for response
	Examination report under AT-C 205	SOC 1 report under AT-C 320 and SOC 1 Guide		
4. Code of ethics	X		Controls provide reasonable assurance that the service organization's (financial intermediary's) code of ethics has been: » formally documented, which includes steps/procedures to identify, research, and report exceptions and documentation of timely resolution; » approved by the board (or other appropriate governing body); » communicated to, and acknowledged by, employees in a timely manner; and » monitored by the compliance department (or other similar internal organization).	The service organization should have a code of ethics that contains provisions in accordance with applicable regulatory requirements.
5. Information security program	X	X	Controls provide reasonable assurance that the service organization's information security program has been: » formally documented, which includes steps/procedures to identify, research, and report exceptions and documentation of timely resolution; » approved by the board (or other appropriate governing body); » communicated to, and acknowledged by, employees in a timely manner; and » monitored by the compliance department (or other similar internal organization).	The service organization should have an information security policy that contains provisions such as: » definition of proprietary, nonpublic, or confidential information; » formal response program for incidents of unauthorized access to, or use of, information; » service organization's approach to privacy as it relates to its operations; » laptop or portable device security; and » impact on, and applicability to, subservice organizations (e.g., third parties, subcontractors). Controls should address process such as: » monitoring compliance with applicable laws and regulations; and » employee awareness and training.

Table 2: Control Areas of Focus 4–17 *continued*

Control area	Potential reporting mechanism		Control objective	Consideration for response
	Examination report under AT-C 205	SOC 1 report under AT-C 320 and SOC 1 Guide		
6. Anti–money laundering (AML) and the prevention of terrorist financing program	X		Controls provide reasonable assurance that the service organization's anti–money laundering and prevention of terrorist financing program has been: » formally documented, which includes steps/procedures to identify, research, and report exceptions and documentation of timely resolution; » approved by the board (or other appropriate governing body); » communicated to, and acknowledged by, employees in a timely manner; and » monitored by the compliance department (or other similar internal organization).	The service organization should have an anti–money laundering and prevention of terrorist financing program that contains provisions in accordance with applicable regulatory requirements and following the globally recognized principles for compliance risk management and oversight, including: » firmwide approach to BSA/AML/OFAC compliance risk management and oversight; » independence of compliance staff; » compliance monitoring and evidence of annual independent testing of the program; and » board and senior management responsibilities for compliance risk management and oversight.
7. Document retention and recordkeeping	X		Controls provide reasonable assurance that the service organization's document retention and recordkeeping guidelines have been: » formally documented, which includes steps/procedures to identify, research, and report exceptions and documentation of timely resolution; » approved by the board (or other appropriate governing body); » communicated to, and acknowledged by, employees in a timely manner; and » monitored by the compliance department (or other similar internal organization).	The service organization should have a document retention and recordkeeping policy that contains provisions in accordance with applicable regulatory requirements, such as: » time periods for retention of documents; » document destruction protocols; » tracking of changes to documents and the prevention of unintended alterations to records; and » provisions to put a "hold" on the records. Controls should consider addressing the processes for: » how historical accounting records (since inception) are retained; » document destruction practices; » tracking of changes to documents and the prevention of unintended alterations to records; » the location of records (e.g., image system, microfilm, boxes); and » subservice organization (e.g., subcontractor/vendor) compliance.

Table 2: Control Areas of Focus 4–17 *continued*

Control area	Potential reporting mechanism		Control objective	Consideration for response
	Examination report under AT-C 205	SOC 1 report under AT-C 320 and SOC 1 Guide		
8. Security master setup and maintenance	X	X	Controls provide reasonable assurance that new mutual funds and changes to existing funds are authorized and entered in the security master file in a complete, accurate, and timely manner.	Controls should consider addressing the processes for: » setting up and modifying key fund data that are maintained in the security master file (e.g., new funds, changes to prospectus and fund policies); » reviewing the setup and maintenance activity to ensure that it was authorized and performed completely and accurately; » monitoring and escalation process to notify the user entity (fund complex) management of those matters that require judgment (exceptions and overrides); and » oversight of subservice organizations (e.g., complementary user entity control considerations at subaccounting platforms where these controls may be performed).

Table 2: Control Areas of Focus 4–17 *continued*

Control area	Potential reporting mechanism		Control objective	Consideration for response
	Examination report under AT-C 205	SOC 1 report under AT-C 320 and SOC 1 Guide		
9. Transaction processing—financial and nonfinancial (e.g., account setup and maintenance)	X	X	**Financial:** Controls provide reasonable assurance that: » specified transactions and adjustments, including as-of transactions, are authorized; processed completely, accurately, and in a timely manner; and are effected at the proper price; » specified transactions meet requirements contained in mutual fund prospectuses and statements of additional information governing shareholder transactions; and » dividends and capital gain distributions are recorded and paid or reinvested, based on authorized amounts, in a complete, accurate, and timely manner.	**Financial:** Controls should consider addressing the processes for: » transactions received through various communication channels (e.g., phone, fax, internet, mail); » mid-month account closeout (how investor accounts are credited with dividends); » executing transactions in accordance with prospectus and regulatory requirements (including exception identification, escalation, and resolution). Examples include, but are not limited to: » complying with requests received from fund complexes under Securities and Exchange Commission (SEC) Rule 22c-2; » complying with fund money market policies and guidelines under SEC Rule 2a-7; » timeliness of transaction processing (e.g., SEC Rule 22c-1); » fund-initiated events (e.g., paying out gains and dividends, correctly applying net asset values [NAVs]); » customer-initiated trades (e.g., buy, sell, exchange); and » corrective processing (as-of activity). » compensation activity (e.g., Rule 12b-1 fees, commissions, contingent deferred sales charges (CDSCs), redemption fees); and » oversight of subservice organizations (e.g., complementary user entity control considerations at subaccounting platforms where these controls may be performed).

Table 2: Control Areas of Focus 4–17 *continued*

Control area	Potential reporting mechanism		Control objective	Consideration for response
	Examination report under AT-C 205	SOC 1 report under AT-C 320 and SOC 1 Guide		
9. Transaction processing—financial and nonfinancial (e.g., account setup and maintenance) (continued)	X	X	**Nonfinancial:** Controls provide reasonable assurance that beneficial owner accounts have been: » monitored for compliance with the specified terms or provisions contained in mutual fund prospectuses and statements of additional information or other governing documents.	**Nonfinancial:** Controls should consider addressing the processes for: » coordination of account openings, including gathering relevant information to determine that application is "in good order"; » communication protocols between the user entity (fund complex) and the service organization, including but not limited to: » account establishment and maintenance; » tax (e.g., application of tax status, tax forms, and remitting of withholding); » proxy activities; and » oversight of subservice providers (e.g., complementary user entity control considerations at subaccounting platforms where these controls may be performed).

Table 2: Control Areas of Focus 4–17 *continued*

Control area	Potential reporting mechanism		Control objective	Consideration for response
	Examination report under AT-C 205	SOC 1 report under AT-C 320 and SOC 1 Guide		
10. Cash and share reconciliations	X	X	Controls provide reasonable assurance that: » accounts are reconciled, and exceptions are identified, researched, and resolved in a complete, accurate, and timely manner, and » beneficial owner accounts are reconciled at a CUSIP level between the subaccounting system, the brokerage platform, and the omnibus position held on the transfer agent system and that exceptions are identified, researched, and resolved in a complete, accurate, and timely manner.	Controls should consider addressing the processes for: » daily reconciliation: » cash accounts, and » beneficial owner share positions at a CUSIP level between the subaccounting system, the brokerage platform, and the omnibus position held on the transfer agent system; » guidelines (materiality levels) for exception identification; » monitoring by management; and » oversight of subservice organizations (e.g., complementary user entity control considerations at subaccounting platforms where these controls may be performed).
11. Lost and missing security holders	X		Controls provide reasonable assurance that the service organization has policies and procedures relating to reporting and remitting abandoned property to the states as appropriate and such policies and procedures: » are formally documented; » ensure that accounts are monitored to determine when property becomes deemed abandoned and reported to the state(s); » are implemented in a manner reasonably designed to ensure complete, accurate, and timely reporting and remittance of abandoned property to the appropriate state; and » are reviewed on an ongoing basis to ensure that they remain current.	The service organization should: » have a process to monitor accounts for purposes of federal and state reporting of lost security holders/abandoned property; » ensure that: » accounts are monitored to determine when an account must be deemed abandoned by law, » required searches are performed in a timely fashion, and » the proper reporting of such account to the states takes place as required by law. » have a process for remitting abandoned property to the appropriate state; and » conduct oversight of subservice organizations (e.g., complementary user entity control considerations at subaccounting platforms where these controls may be performed).

Table 2: Control Areas of Focus 4–17 *continued*

Control area	Potential reporting mechanism		Control objective	Consideration for response
	Examination report under AT-C 205	SOC 1 report under AT-C 320 and SOC 1 Guide		
12. Shareholder communications	X	X	Controls provide reasonable assurance that shareholder communications prepared by the fund are distributed in accordance with the financial intermediary's shareholder records in a complete, accurate, and timely manner. Controls provide reasonable assurance that shareholder statements and tax reporting are distributed in accordance with the financial intermediary's shareholder records in a complete, accurate, and timely manner.	Controls should consider addressing the processes for: » delivery—how various items are shipped or communicated (including electronically), such as: » prospectuses, » shareholder reports, » statements (confirmations, monthly, quarterly, and year-end communications), and » tax reporting (e.g., information reporting and withholding/ remittance to shareholders and the Internal Revenue Service [IRS]); » management monitoring; and » oversight of subservice organizations (e.g., complementary user entity control considerations at subaccounting platforms and print mail vendors where these controls may be performed).
13. Subaccount billing, invoice processing	X	X	Controls provide reasonable assurance that amounts billed for shareholder servicing by financial intermediaries have been calculated and applied in accordance with the terms of the agreement between the service organization and user entity (fund complex or its affiliate) and are complete, accurate, and timely.	Controls should consider addressing the processes for: » verification of fee amounts; » comparing and ensuring agreement between the billing/invoicing information and the number of accounts on the underlying books and records; » production and distribution of invoices; » management monitoring; and » oversight of subservice organizations (e.g., complementary user entity control considerations at subaccounting platforms where these controls may be performed).

Table 2: Control Areas of Focus 4–17 *continued*

Control area	Potential reporting mechanism		Control objective	Consideration for response
	Examination report under AT-C 205	SOC 1 report under AT-C 320 and SOC 1 Guide		
14. Fee calculations	X	X	Controls provide reasonable assurance that: » initial sales charges, CDSCs, 12b-1 fees, and redemption fees have been calculated and applied completely, accurately, and in a timely manner in accordance with mutual fund prospectus and statement of additional information requirements.	Controls should consider addressing the processes for: » capturing all fee types from the prospectus or other selling document (e.g., considering class of shares, rights of accumulation, letters of intent, account aggregation, concurrent purchases, waivers, "free shares," share aging, lot tracking, reinvested shares, etc.); » verification of fee amounts; » comparing and ensuring agreement between the information and the underlying books and records; » grouping (e.g., asset based, account based) of fee types, if applicable; » production and distribution of invoices; » management monitoring; and » oversight of subservice organizations (e.g., complementary user entity control considerations at subaccounting platforms where these controls may be performed).

Table 2: Control Areas of Focus 4–17 *continued*

Control area	Potential reporting mechanism		Control objective	Consideration for response
	Examination report under AT-C 205	SOC 1 report under AT-C 320 and SOC 1 Guide		
15. Information technology (including internet and VRU)	X	X	Controls provide reasonable assurance that: » logical access to programs, data, and computer resources is restricted to authorized and appropriate users, and such users are restricted to performing authorized and appropriate actions; » physical access to computer and other resources is restricted to authorized and appropriate personnel; » changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances; » network infrastructure is configured as authorized to (1) support the effective functioning of application controls to result in valid, complete, accurate, and timely processing and reporting of transactions and balances and (2) protect data from unauthorized changes; » application and system processing are authorized and executed in a complete, accurate, and timely manner, and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete, accurate, and timely manner; » data transmissions between the service organization and its user entities and other outside entities are from authorized sources and are complete, accurate, secure, and timely; and » data are backed up regularly and are available for restoration in the event of processing errors or unexpected processing interruptions.	Controls should consider addressing the processes for: » application changes, including management oversight; » downloads of data and interfaces with external parties; » connectivity (e.g., Are dedicated lines established for certain user entities?); » network security; » virus protection/propagation procedures; » use and security of portable devices; » oversight of subservice organizations (e.g., complementary user entity control considerations at subaccounting platforms where these controls may be performed); and » physical security: » security infrastructure, » entry point access (manual or electronic), and » access restrictions within various facilities.

Table 2: Control Areas of Focus 4–17 *continued*

Control area	Potential reporting mechanism		Control objective	Consideration for response
	Examination report under AT-C 205	SOC 1 report under AT-C 320 and SOC 1 Guide		
16. Business continuity/ Disaster recovery program	X		Controls provide reasonable assurance that business continuity and disaster recovery plans have been: » formally documented; » approved by the board (or other appropriate governing body); » communicated to employees in a timely manner; » compliance with the business continuity/disaster recovery program is monitored by the compliance department (or other similar internal organization); » designed to identify, research, and report exceptions and that any resolution is documented in a timely manner: » data and systems are backed up regularly and retained off-site; » information technology hardware and software issues are monitored and resolved in a timely manner; and » plans are fully tested, including testing for data and systems recoverability.	The service organization should have business continuity and disaster recovery plan(s) that contain provisions in accordance with applicable regulatory requirements. The plan(s), procedures, and controls should consider addressing: » the scenarios contemplated in the plan(s) and other general provisions; » testing and training plan(s), including timetables (e.g., annual, semiannual); » capabilities (i.e., "hot" site or "cold" site) and proximity of off-site locations; » expected recovery time frame for key systems and processes; » communicating with outside parties (e.g., fund management) in the event of an emergency; » power backup; » oversight of subservice organizations (e.g., complementary user entity control considerations at subaccounting platforms where these controls may be performed); and » other considerations associated with: » systems; » people; » facilities; and » various interruption scenarios: scenarios should contemplate items ranging from gas leaks and natural disasters to loss of key personnel.

Table 2: Control Areas of Focus 4–17 *continued*

Control area	Potential reporting mechanism		Control objective	Consideration for response
	Examination report under AT-C 205	SOC 1 report under AT-C 320 and SOC 1 Guide		
17. State of sale reporting (for blue sky purposes)	X		Controls provide reasonable assurance that sales by state are reported to the user entity (fund complex or its agent) in a complete, accurate, and timely manner.	Controls should consider addressing the processes for: » verification that sales by state are completely, accurately, and in a timely manner reported to the fund or its blue sky agent; » management monitoring; and » oversight of subservice organizations (e.g., complementary user entity control considerations at subaccounting platforms where these controls may be performed).

IV. Glossary

Introduction

AICPA (American Institute of Certified Public Accountants)

The nonprofit professional organization of certified public accountants in the United States. The AICPA represents the CPA profession nationally regarding rulemaking and standard-setting and serves as an advocate before legislative bodies, public interest groups, and other professional organizations. The AICPA develops standards for audits of private companies and other services by CPAs, provides educational guidance materials to its members, develops and grades the Uniform CPA Examination, and monitors and enforces compliance with the profession's technical and ethical standards.

Areas of focus

The 17 major categories addressed in the FICCA framework, including three information areas and 14 control areas. The information areas provide critical information and context about the intermediary's business environment. Any controls related to the information areas are not typically tested by the practitioner, nor are they covered by management's assertion. The control areas each include a description of the controls that the financial intermediary has implemented. The practitioner tests these controls to determine whether they were suitably designed and are operating effectively to achieve the related control objectives.

Control activities

Control activities, or controls, are the policies and procedures that help ensure that management directives are carried out.

Control area

In the context of the FICCA framework, this term refers to the 14 areas of focus for which the financial intermediary has implemented controls. The practitioner tests these controls to determine whether they were suitably designed and are operating effectively to achieve the related control objectives.

Controls also may exist in the three information areas of focus. These controls are not typically tested by the practitioner, nor are they covered by management's assertion.

Control environment

The control environment sets the tone of an organization, influencing the control consciousness of its staff. It is the foundation for all other components of internal control, providing discipline and structure.

Control objective

The aim or purpose of controls implemented by the financial intermediary. The practitioner tests these controls to determine whether they were suitably designed and are operating effectively to achieve the related control objective. Descriptions of the tests performed, and the results of the tests, are included in the practitioner's report.

Financial intermediary

An entity such as a broker-dealer that sells (distributes) mutual fund shares and provides services to end investors (customers or shareholders). In an examination attestation engagement performed on a financial intermediary that provides services to a mutual fund, the financial intermediary is also known as the *service organization*.

Fund company (complex, sponsor)

A group of mutual funds, each with a typically distinct investment objective, that is managed and made available for sale/distribution by the same company. In an examination attestation engagement, the fund company that uses the services of a financial intermediary is known as the *user entity*.

Information area

In the context of the FICCA framework, this term refers to the three areas of focus for which the financial intermediary provides background information about its business environment. The financial intermediary typically does not identify controls related to these areas. This information is considered "other information" and is not covered by the practitioner's report or management's assertion.

Management's assertion

A written statement provided by management of the financial intermediary about whether the intermediary's controls were suitably designed and are operating effectively to achieve the control objectives.

Operating effectiveness

A control is determined to be operating effectively if it was suitably designed and is executed as designed. (This includes such matters as whether the control is performed at the predetermined frequency, whether the persons performing the control possess the necessary authority and competence, and the consistency with which the control is applied.)

Practitioner

The AICPA-designated term for the CPA/firm performing an examination attestation engagement that is related to the FICCA framework.

Service organization

The AICPA-designated term for the financial intermediary organization in the context of an examination attestation engagement that is related to the FICCA framework.

SOC 1 report

A report resulting from an examination engagement performed under the AT-C 320 report, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting,* of the attestation standards**.** This report is intended to meet the needs of management of the service organization, user entities, and auditors of the user entities' financial statements (user auditors) as they evaluate the effect of the controls at the service organization on the user entities' financial statements. There are two types of reports:

- **Type 1:** Report on the fairness of the presentation of management's description of the service organization's system and the suitability of the design of the controls to achieve the related control objectives as of a specified date.
- **Type 2:** Report on the fairness of the presentation of management's description of the service organization's system and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period.

The use of these reports is restricted to the management of the service organization, user entities of the service organization, and user auditors.

SOC 2 report

A report resulting from an examination engagement performed under AT-C 205 *Examination Engagements* of the attestation standards and the AICPA guide, *Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.* The report is intended to meet the needs of a broad range of users that need detailed information and assurance about the internal control at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems. This report is intended for use by stakeholders (e.g., customers, regulators, business partners, suppliers, directors) of the service organization who have a thorough understanding of the service organization and its controls. These reports can form an important part of stakeholders' oversight of the financial intermediary; vendor management program; internal corporate governance and risk management processes; and regulatory oversight. There are two types of reports:

- **Type 1:** Report on management's description of a service organization's system and the suitability of the design of controls to achieve the related control objectives as of a specified date.
- **Type 2:** Report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls to achieve the related control objectives included in the description throughout a specified period.

Subservice organization

The AICPA-designated term for a third-party vendor organization providing services to the financial intermediary organization (service organization) in the context of an examination attestation engagement that is related to the FICCA framework.

Transparency data

Information that may be received by fund complexes, typically in electronic form, describing general account attributes and activity of fund shareholders holding shares through an intermediary omnibus account.

User entity

The AICPA-defined term for a fund complex in the context of an examination attestation engagement that is related to the FICCA framework.

General

Statement of Position 07-2 Attestation Engagements That Address Specified Compliance Control Objectives and Related Controls at Entities That Provide Services to Investment Companies, Investment Advisers, or Other Service Providers

The Statement of Position (SOP) 07-2 is an interpretative publication and represents the recommendations of the Chief Compliance Officers Task Force of the AICPA Auditing Standards Board regarding the application of attestation engagement standards primarily to examination engagements in which a practitioner reports on the suitability of the design and operating effectiveness of a service provider's controls in achieving specified compliance control objectives.

An examination engagement following SOP 07-2 is performed in accordance with AT-C 205. Examination attestation engagements resulting in a practitioner's report are guided by SOP 07-2 and AT-C 205.

Third-party vendor organization

A subservice organization (e.g., subservice provider or subcontractor) used by a service organization (e.g., financial intermediary) to perform certain services provided to the user entity (e.g., fund complex) that are likely to be relevant to the user entity's internal controls for areas of focus included in the framework.

Risk governance program

Internal control

The set of policies and procedures designed, implemented, and maintained by governance, management, and other personnel charged with providing reasonable assurance about the achievement of the entity's objectives regarding the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations.

Risk assessment

The entity's process for identifying and analyzing risks relevant to achieving its objectives, as well as forming a basis for determining how those risks should be managed.

Code of ethics

Code of ethics

A guide that includes principles designed to help professionals conduct business honestly and with integrity.

Anti–money laundering (AML) and the prevention of terrorist financing program

Anti–money laundering (AML)

A set of procedures, laws, or regulations designed to prevent, detect, and report money laundering activities. Money laundering generally involves concealing the source of money that has been obtained through illegitimate means.

Bank Secrecy Act (BSA)

Congress passed the Bank Secrecy Act (BSA) in 1970 as the first law to fight money laundering in the United States. The BSA requires businesses to keep records and file reports that are determined to have a high degree of usefulness in criminal, tax, and regulatory matters. The documents filed by businesses under the BSA requirements are heavily used by law enforcement agencies, both domestic and international, to identify, detect, and deter money laundering whether it is in furtherance of a criminal enterprise, terrorism, tax evasion, or other unlawful activity.

Customer Due Diligence (CDD) Rule

The Customer Due Diligence (CDD) Rule, part of the BSA, requires the identification and verification of the ultimate beneficial owners of certain legal entity customers. The rule is intended to help financial institutions operating in the United States to more clearly identify customers and gain greater insight into business relationships.

Office of Foreign Assets Control (OFAC)

The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy, or economy of the United States.

Security master setup and maintenance

Complementary user entity controls

Controls that management of the service organization assumes, in the design of its system, will be implemented by the user entity and that are necessary to achieve the control objectives stated in management's description of the service organization's system. This is a term defined by AT-C 320 audit standards.

Security master file

The records on the brokerage or intermediary platform containing descriptive security data, such as security name, type, eligibilities, and fee schedules, as defined in fund prospectuses and processing rules.

Subaccounting platform

Recordkeeping platform used by the subaccounting agent who assists financial intermediaries in maintaining mutual fund shareholder account and transaction records.

Transaction processing—financial and nonfinancial (e.g., account setup and maintenance)

Account closeout

When an account is closed or terminated by the shareholder.

As-of transaction

A transaction that receives an effective date prior to its trade (processing) date.

Beneficial owner

Term for the underlying investor who owns fund shares in an account held on the intermediary's books and records. The shares, in turn, are held in an aggregate omnibus account registered to the intermediary firm on the fund transfer agent's recordkeeping system.

Mutual fund prospectus

The official document that describes an investment company to prospective investors. The prospectus contains information required by the SEC, such as investment objectives and policies, risks, services, and fees.

Statement of additional information (SAI)

The supplementary document to a prospectus that contains more detailed information about a mutual fund; also known as Part B of the prospectus.

Cash and share reconciliations

Brokerage platform

Platform used by a financial intermediary to provide mutual fund shareholder servicing functions.

CUSIP

A means of uniformly describing and identifying all stocks and registered bonds in numeric form developed by the Committee on Uniform Securities Identification Procedures (CUSIP).

Omnibus position

An omnibus position on a mutual fund's primary transfer agency system representing the aggregate share balance of multiple investors. Any underlying investor information provided by intermediaries after transaction processing may be limited (partial disclosure) and currently is not incorporated in the fund's primary transfer agent recordkeeping system.

Transfer agent

The internal or external organization that a mutual fund uses to process shareholder transactions, maintain related records, provide relevant shareholder communications and reporting, and service investor accounts.

Lost and missing security holders

Abandoned property

Assets such as cash, stocks, bonds, mutual funds, uncashed checks, land, life insurance policies, and the contents of safe deposit boxes that have been turned over to the state after prescribed periods of inactivity.

Subaccount billing, invoice processing

Subaccount billing

Fees calculated and billed to mutual fund complexes by financial intermediaries for shareholder servicing, recordkeeping, and reporting functions.

Fee calculations

Contingent deferred sales charge (CDSC)

A fee imposed by some mutual funds when shares are redeemed (sold back) during the first few years of ownership. CDSCs typically decline over a specified number of years, eventually falling to zero. Under specific prospectus provisions, the CDSC is triggered if the investor redeems fund shares before a given number of years of ownership (typically six to eight years for Class B shares).

Free shares

Acquired shares that are not subject to a commission (e.g., shares are no longer, or were never, subject to front- or back-end sales charges).

Initial sales charges

Amounts charged for the sales of some mutual fund shares. Charges may vary depending on the amount invested and the fund chosen. By regulation, mutual fund sales charges are capped.

Letter of intent (LOI)

A privilege allowing individual investors who intend to invest an amount in excess of a load fund's breakpoint within a designated time period to pay a reduced sales charge that would have been applicable had such an investment been made in a single lump sum.

Lot tracking

Recording of the investor's share purchase and redemption activity to enable the calculation and tax treatment for compliance and reporting upon sale.

Redemption fees

The amount a shareholder may pay to the fund when redeeming fund shares within a specified period of time. This fee is to cover the costs associated with the redemption and to deter market timing activity.

Rights of accumulation

An account privilege that allows individual investors or groups of related investors to combine their account balances and share purchases (within the same fund family) when calculating a sales load rate in order to receive the appropriate discounted sales charge in accordance with the fund's prospectus policies.

Share aging

Tracking of the investor's share purchase and sale activity for load funds so the appropriate fees and sales charges are applied based on purchase date and sale date.

Share class

Many mutual funds offer investors different types, or classes, of shares (e.g., Class A, Class C, institutional shares). Each class will invest in the same portfolio of securities and will have the same investment objectives and policies, but each class will have different shareholder profiles and services and/or distribution arrangements with different fees and expenses and, therefore, different expense ratios. A multiclass structure offers investors the ability to select a fee and expense structure that is most appropriate for their investment goals (including the time they expect to remain invested in the fund).

12b-1 fee

A mutual fund fee, named for the SEC rule that permits it, used to pay distribution costs and administrative service fees such as compensation to financial advisers for initial and ongoing assistance. If a fund has a 12b-1 fee, it will be disclosed in the fee table of the fund's prospectus.

Waiver

When an investment adviser, administrator, or distributor decides to temporarily forgo all or part of the management fee, administration fee, or 12b-1 fee paid by the mutual fund.

Information technology (including internet and VRU)

VRU (voice response unit)

An automated telephone system that enables shareholders to obtain net asset values, performance information, and account information. Certain systems also may enable shareholders to make exchanges, redemptions, or additional investments.

State of sale reporting (for blue sky purposes)

Blue sky reporting

State regulations designed to protect investors against securities fraud by requiring sellers of new issues to register their offerings and provide financial details.

Internal Control Reporting Standards Reference Guide

Statement on Standards for Attestation Engagements (SSAE)

Refers to the Statement on Standards for Attestation Engagements developed and updated periodically by the AICPA, most recently as SSAE Number 18, effective May 2017. The FICCA framework was developed and has been maintained to align with clarified attestation standard AT-C 205 *Attestation Engagements* under SSAE-18.

V. Sample Report of Independent Accountants and Management Assertion

Introduction

The following pages present an example of a report by an independent accountant (known as a *practitioner* in the attestation standards) and an assertion by management of a financial intermediary (*service organization*) that would be provided in connection with an examination attestation engagement related to the FICCA framework. The exact language in the practitioner's report and management's assertion for an engagement may vary. In the following example, the practitioner is reporting on management's assertion under AT-C Section 205, *Examination Engagements*. Independent practitioners are responsible for complying with their professional standards, and those standards address the form and content of a practitioner's report.

Section 1: Report of independent accountants: The auditor expresses an opinion on whether management's assertion is fairly stated. The practitioner's opinion is based on the practitioner's examination, which includes obtaining an understanding of and evaluating the suitability of the design and operating effectiveness of the controls intended to achieve the specified control objectives. The specific controls tested, and the nature, timing, and results of those tests, are presented in a document that is part of the practitioner's report. The practitioner's report is addressed to management of the intermediary and is intended for use by management of the intermediary and fund complexes that have contracted with the financial intermediary to provide shareholder servicing and recordkeeping functions.

Section 2: Management assertion: Management of the intermediary asserts that control objectives and related controls were established and that those controls were suitably designed throughout a specified period to provide reasonable assurance that the control objectives would be achieved. Management of the intermediary also asserts that the controls operated effectively to provide reasonable assurance that the specified control objectives were achieved throughout the specified period. The control objectives and related controls are the responsibility of management and are presented in a document that accompanies the assertion (Appendix A). The specific control objectives and related controls included in the appendix would incorporate the 14 control areas of focus detailed in the FICCA framework.

Report of Independent Accountants

To the Management of [*Name of service organization*]:

Scope

We have examined the assertion by management of [*Name of service organization*] pertaining to its controls related to the financial intermediary functions [*identify the functions* (*can be the 14 control areas within the framework*)] that [*Name of service organization*] performs for funds (*user entities*). Management's assertion is included in the accompanying document titled "Management's Assertion on the Control Objectives and Related Controls over Financial Intermediary Functions" and states the following:

- The controls, as established by [*Name of service organization*]'s management and described in Appendix A [*Name of service organization*] "Control Objectives and Related Controls" (Appendix A), were suitably designed and implemented throughout the period [date] to [date] to provide reasonable assurance that the control objectives described therein would be achieved, if those controls were complied with satisfactorily and user entities applied the complementary user entity controls assumed in the design of [*Name of service organization*]'s controls throughout the period [*date*] to [*date*].
- The controls described in Appendix A operated effectively to provide reasonable assurance that the control objectives described therein were achieved throughout the period [*date*] to [*date*], if user entities applied the complementary user entity controls assumed in the design of [*Name of service organization*]'s controls throughout the period [*date*] to [*date*].

Management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

As indicated in management's assertion, [*Name of service organization*]'s control objectives related to [*identify the areas of focus or subject matter of control objectives and related controls addressed in another practitioner's report*] are addressed in another examination report issued by an independent accounting firm. Because these control objectives are excluded from management's assertion and description (Appendix A), the scope of our work did not include examining the design, implementation, or operating effectiveness of controls to achieve those control objectives, and we do not express an opinion thereon.

[*Name of service organization*] uses [*Name of subservice organization*] to [*identify the function(s) provided by the subservice organization*]. Management's assertion addresses only the control objectives and related controls of [Name of service organization] and excludes the control objectives and related controls of [*Name of subservice organization*]. Our examination did not extend to controls of [*Name of subservice organization*].

Our Responsibilities

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Our examination was limited to examining the specified control objectives and related controls and did not consider any other control objectives or controls that may be relevant to management's or the user entities' internal control over financial intermediary functions. The effectiveness of controls to achieve the specified control objectives is subject to inherent limitations, and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any evaluations of effectiveness to future periods is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls or the failure to make needed changes to the system or controls may alter the validity of such evaluations.

Other Information Provided by [Client Name]

The information included in the section titled "Other Information Provided by [*Name of service organization*]" is presented by management of [*Name of service organization*] to provide additional information and is not covered by management's assertion in Section 2. The "Other Information Provided by [*Name of service organization*]" includes management's description of FICCA information areas of focus 1–3 and areas of focus covered by another independent accountant's report. Information about the company's [*additional information*] has not been subjected to the procedures applied in the examination of management's assertion and of the suitability of the design and operating effectiveness of controls to achieve the specified control objectives stated in management's assertion, and, accordingly, we express no opinion on it.

Opinion

In our opinion, management's assertion in Section 2 referred to above is fairly stated in all material respects.

Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those tests, are listed in Appendix A.

Restricted Use

This report, including the description of tests of controls and results thereof in Appendix A, is intended solely for the information and use of management of [*Name of service organization*] and the user entities of the [*Name of service organization*]'s [*identify the functions the service organization performs for user entities*] throughout the period [*date*] to [*date*] and is not intended to be and should not be used by anyone other than these specified parties.

[*Signature*]

[*Date*]

Sample Management Assertion[10]

[*Name of service organization*] provides certain financial intermediary functions to fund complexes (user entities). Management of [*Name of service organization*] has prepared this assertion following guidelines provided in *Financial Intermediary Controls and Compliance Assessment Engagements*, August 2020 (FICCA framework), published by the Investment Company Institute. Management has established specified control objectives related to control areas of focus identified in the FICCA framework and related controls to achieve these specified control objectives. These specified control objectives and related controls are the responsibility of management of [*Name of service organization*] and are presented in Appendix A [*Name of service organization*]'s "Control Objectives and Related Controls" (Appendix A). The areas of focus addressed by this assertion and the areas of focus that are addressed in another practitioner's report are identified in a section titled "Other Information Provided by [*Name of service organization*]." For each control area of focus included in our assertion, management established specified control objectives and related controls. We, as members of management, are responsible for establishing the specified control objectives and related controls and for the suitability of the design and operating effectiveness of the controls.

Management's description in Section 2 identifies areas of focus in the FICCA framework that are excluded from management's description or addressed in another practitioner's report on [*Name of service organization*]'s controls. Additionally, [*Name of service organization*] uses the following subservice organizations:

[*Name of subservice organization*], [*identify the functions the subservice organization performs for user entities*].

Management's assertion includes only those specified control objectives and related controls of [*Name of service organization*] and does not include specified control objectives and related controls of subservice organizations.

We have evaluated whether [*Name of service organization*]'s controls were suitably designed and operating effectively to achieve the specified control objectives throughout the period [*date*] to [*date*]. The criteria against which the controls were evaluated are the specified control objectives. Based on our evaluation, we assert the following:

- The controls established by [*Name of service organization*]'s management and described in Appendix A were suitably designed and implemented throughout the period [*date*] to [*date*] to provide reasonable assurance that the specified control objectives described therein would be achieved, if those controls were complied with satisfactorily and user entities applied the complementary user entity controls assumed in the design of [*Name of service organization*]'s controls throughout the period [*date*] to [*date*].
- The controls established by [*Name of service organization*]'s management and described in Appendix A operated effectively to provide reasonable assurance that the control objectives described therein were achieved throughout the period [*date*] to [*date*], if user entities applied the complementary user entity controls contemplated in the design of [*Name of service organization*]'s controls throughout the period [*date*] to [*date*].

[*Signature*]

[*Date*]

[10] In the event that management identifies a material misstatement or deviation from the criteria, the practitioner should follow the guidance in paragraphs 78–79 of AT-C Section 205, *Examination Engagements* (*AICPA Professional Standards*, 2017, vol. 1), and report directly on the subject matter, not on the assertion.

Appendix A: Template for Describing Test of Controls and Results

The following template (referred to as "Control Objectives and Related Controls" [Appendix A] in the sample report) is intended to help organize the controls applicable to each of the 14 control areas and is included as part of the examination report.[11] Fund complexes seek independent assurance that the intermediary has established controls and that those controls are operating as intended as part of management's assertions. Management should complete the "Controls" column of the template and submit with its assertions. The practitioner is responsible for providing its test procedures and results as part of the practitioner's report.

Control areas/Control objectives	Controls	Test procedures	Test results
4. Code of ethics			
5. Information security program			
6. Anti–money laundering (AML) and the prevention of terrorist financing program			
7. Document retention and recordkeeping			
8. Security master setup and maintenance			
9. Transaction processing—financial and nonfinancial (e.g., account setup and maintenance)			
10. Cash and share reconciliation			
11. Lost and missing security holders			
12. Shareholder communications			
13. Subaccount billing, invoice processing			
14. Fee calculations			
15. Information technology (including internet and VRU)			
16. Business continuity/disaster recovery program			
17. State of sale reporting (for blue sky purposes)			

[11] If an area of focus is not covered by the examination attestation engagement, the service organization (financial intermediary) should indicate "Not applicable to this engagement" in the "Controls" column.

VI. Mapping Template for Control Reports

Relationship of [Intermediary Name]'s Examination Attestation Engagement Reports to the Financial Intermediary Controls and Compliance Assessment (FICCA) Framework

[*Intermediary name*] has engaged [*Audit firm name*] to report on its control and compliance environment through one or more examination attestation engagements. ICI's FICCA framework covers 14 control areas of focus for which fund complexes seek independent assurance that the intermediary has established controls and that those controls are operating effectively. Fund complexes expect annual reporting on these control areas (areas of focus 4–17).[12]

The following template is intended to help fund complexes determine, for each of the 14 control areas of focus, whether it is covered by a SOC 1 report under AT-C 320 and the SOC 1 Guide, a SOC 2 report under AT-C 205 and the SOC 2 Guide, or the report resulting from an examination attestation engagement performed under AT-C 205. For each of the areas of focus covered (14 control areas and three information areas), the mapping template indicates the recommended sources of practitioner's reports or other information.

The financial intermediary should complete the mapping by placing a check mark (☑) in the column indicating the report in which the area of focus is addressed.[13] Where the financial intermediary has oversight over a subservice organization performing activities within a control area of focus (e.g., transaction processing) and where a separate practitioner's report for the subservice organization is provided as part of the FICCA framework response, the intermediary should place a separate check mark in the appropriate column for each of the practitioner's reports addressing the related area of focus.

[12] Areas of focus 1–3 are not controls and, therefore, are not within the scope of the practitioner's report.

[13] If an area of focus is not covered by a practitioner's report, leave that row blank.

Investment Company Institute's FICCA framework areas of focus	Reporting used
Section 1: Information areas 1–3	
1. Management reporting (quality control)	Information provided to fund sponsor either outside of practitioner's report(s) or as other information
2. Risk governance program	Information provided to fund sponsor either outside of practitioner's report(s) or as other information
3. Third-party oversight	Information provided to fund sponsor either outside of practitioner's report(s) or as other information

Investment Company Institute's FICCA framework areas of focus	Examination report under AT-C 205 for the period [date] to [date]	SOC 1 report under AT-C 320 and the SOC 1 Guide for the period [date] to [date]
Section 2: Control areas 4–17		
4. Code of ethics		
5. Information security program		
6. Anti–money laundering (AML) and the prevention of terrorist financing program		
7. Document retention and recordkeeping		
8. Security master setup and maintenance		
9. Transaction processing—financial and nonfinancial (e.g., account setup and maintenance)		
10. Cash and share reconciliation		
11. Lost and missing security holders		
12. Shareholder communications		
13. Subaccount billing, invoice processing		
14. Fee calculations		
15. Information technology (Including internet and VRU)		
16. Business continuity/disaster recovery program		
17. State of sale reporting (for blue sky purposes)		

VII. Internal Control Reporting Standards Reference Guide

Common name	AICPA standard	Engagement type	Report includes	Restrictions on the use of the report	Examples
SOC 1	AT-C 320	Reporting on an examination of controls at a service organization relevant to user entities' internal control over financial reporting	» Fairness of the presentation of management's description » Suitability of the design of the service organization's controls » Operating effectiveness of the service organization's controls » Description of the tests performed and the results of those tests » Service auditor's opinion	Management of the service organization, user entities, and the auditors of the user entities' financial statements	AT-C 320 reports
SOC 2	AT-C 205	Reporting on controls at a service organization relevant to security availability, processing integrity, confidentiality, or privacy	» Fairness of the presentation of management's description » Suitability of the design of the service organization's controls » Operating effectiveness of the service organization's controls » Description of the tests performed and the results of those tests	Parties that are knowledgeable about the nature of the service provided by the service organization	Report covering one or more of the five categories of criteria in TSP Section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*
Chief compliance officers controls	AT-C 205	Reporting on a service provider's controls to achieve compliance control objectives relevant to SEC Rules 38a-1 and 206(4)-7	Reporting on the suitability of the design and operating effectiveness of a service provider's controls over compliance that may affect user entities' compliance	Chief compliance officers, management, boards of directors, and independent auditors of the service provider and of the entities that use the services of the service provider	Custody Rule, Financial Intermediary Controls and Compliance Assessment (FICCA) Framework, CCO/38a-1
Agreed-upon procedures (AUP)	AT 201	performing the agreed-upon procedures referred to in paragraph 3 of Statement on Standards for Attestation Engagements (SSAE) 18	» Performing and reporting on the results of agreed-upon procedures related to the controls of a service organization or to transactions or balances of a user entity maintained by a service organization » This report contains a description of the procedures performed by the practitioner and the results of those procedures.	The specified parties that agreed upon the sufficiency of the procedures for their purposes	Equity compensation or specific calculations
Compliance attestation	AT 601	Reporting on controls over compliance with laws and regulations	Reporting on an entity's compliance with the requirements of specified laws, regulations, rules, contracts, or grants	Limited number of parties that established the criteria or can be presumed to understand the criteria	Vendor contract compliance, Reg AB

Common name	AICPA standard	Engagement type	Report includes	Restrictions on the use of the report	Examples
Compliance Program Evaluation Report (CPER)	Statement of Position (SOP) 07-2 in conjunction with AT-C 205	Attestation engagements that address specified compliance control objectives and related controls at entities that provide services to investment companies, investment advisers, or other service providers	Reporting on the suitability of the design and operating effectiveness of the service provider's controls in achieving management's compliance control objectives	Investment companies and investment advisers	Control reports for subadvisers
Rule 204-2(b) and 206(4)-2 reports	AT-C 315	Reporting on an organization's controls to achieve compliance control objectives relevant to SEC Rules 204-2(b) and 206(4)-2	Reporting on management's assertion or management's compliance pursuant to custody of client funds and securities	Management of the service organization and user entities	Books and records reporting; custody reporting

VIII. FICCA Framework Revision History

Version	Date published	General description/Main changes
2.2	August 2020	» Incorporated use of AICPA terminology, including references to documentation under SSAE 18. » Added fund money market policies and guidelines to transaction processing—financial and nonfinancial. » Separated FICCA framework table into two sections based on which areas of focus may be assessed and operationally tested. Those 14 areas of focus are referred to as "control areas" throughout the document. The three that are not typically tested are referred to as "information areas." » Refined field definitions within FICCA framework, including changing "points to consider" to "consideration of response." » Updated potential reporting mechanisms within the framework and related "Mapping Template for Control Reports" to reflect reports from engagements under AT-C 205 or Type 2 SOC 1 under AT-C 320 and the SOC 1 Guide report. Removed explicit references to third-party reporting as redundant, since the reporting mechanisms listed apply to both the service organization and subservice organization. » Expanded glossary. » Added sample Appendix A for management to document controls related to the framework's 14 control areas/control objectives. » Created revision history table.
2.1	December 2015	» Updated references to SSAE 16 and to AT 801 to reflect current AICPA codification. » Three areas of focus, management reporting (quality control), risk governance, and third-party oversight, were clarified. While still part of the FICCA, they were covered neither by the management's assertion nor by practitioner's report. » Added completely to "management description or controls testing" and/or "points to consider" for several control items to comply with AICPA attestation standards. Audit firms use several objectives to assess a control's design and effectiveness, including completeness, accuracy, validity, and restricted access (known as CAVR). » When activities related to an area of focus are outsourced to a third-party service provider (subservice organization), "points to consider" was clarified to address oversight of the subservice providers, as opposed to excluding the area of focus from the final report. » Anti–money laundering and the prevention of terrorist financing program area of focus—added clarifying language related to compliance monitoring and annual independent testing of the program. » Transaction processing area of focus—added clarifying language related to compliance with SEC Rule 22c-1 and 22c-2. » Renamed blue sky reporting area of focus to state of sale reporting (for blue sky purposes) and added clarifying language regarding the role of the intermediary to provide data to the fund or its designated blue sky agent.

Version	Date published	General description/Main changes
2.0	January 2014	» "Overview and objective" section of the matrix: (1) added definitions of key terms; (2) recommended an annual review of the 17 "Areas of Focus." » Removed "financial viability" as an area of focus as it is covered in the intermediary's audited financial statements. » Added "blue sky reporting." » Renamed "sample control objectives" to "management description or controls testing" and determined whether each area of focus should be subject to controls testing or covered in a management narrative. » Streamlined text in "management description or controls testing" and "points to consider" columns to assist intermediaries and practitioners. » Clarified that "points to consider" are representative but may not be all-inclusive of what should be considered in each engagement. » Asserted the need for intermediary flexibility when providing funds with independent assessment of the 17 control areas, either through one comprehensive FICCA report or a combination of attest reporting (e.g., SSAE 16 and FICCA).
1.0	2008	Initial version

INVESTMENT COMPANY INSTITUTE®

WASHINGTON, DC • LONDON • HONG KONG • WWW.ICI.ORG