Third-Party Reporting on Internal Controls

NQR

INSIGHT

Third-Party Reporting on Internal Controls

Today's Agenda

I. Introduction / Session Overview

II. Current Industry Trends

III. SOC Reporting Overview

IV. FICCA Reporting Overview

V. NQR & Audit Report Efficiencies

I. Session Overview – Today's Presenters

David Parks

Dave is a managing director within EY's Consulting Practice. He has over 33 years of experience working with asset management and broker-dealer organizations. During his career, Dave has worked with transfer agent and intermediary operations to design and evaluate internal controls supporting financial, regulatory compliance, and third-party oversight. Dave has performed several SOC reporting and FICCA reporting engagements.

Michael Gentile

Michael is a senior manager within EY's Assurance practice with over 14 years of experience in the financial services industry. He spends the majority of his time working with asset management firms including registered investment advisors and transfer agents. Michael leads SOC 1 and internal control engagements at some of the world's largest institutional investment advisors. He works closely with the FSO SOC Reporting practice leaders and coordinates and teaches SOC training throughout the U.S.

Thomas Rowan

Tom supports all business lines and corporate operations of NQR. He has been involved in the development of NQR's Intermediary INSIGHT service since its inception in 2013, and plays a particularly active role in the management of the Audit Report Review Team. Tom joined NQR in 2010.

I. Session Overview – Presentation Objectives

- Share industry trends that are driving the **evolution and importance of reporting on internal controls** at service providers
- Establish a foundational **understanding of third-party reporting options** available to the AM industry
- Review **auditor practices and trends** when working with service organizations, including attestation frameworks, concepts, methodologies, and testing
- Review **User Organization responsibilities** related to using the report
- Provide an overview of industry drivers and authoritative viewpoints on the importance of third-party reporting in **support of oversight and due diligence**
- Share industry **insights on EY's experience** *(what is working and where improvements are being made)*

II. Current Industry Trends

Trends Driving the Use and Importance of Attestation Reporting

Required Insight on How Third-Party Partners Manage Risk: The type of risks facing the industry are changing rapidly, and competition is becoming more intense. Firms are increasingly looking to third parties to perform operational tasks, and this includes managing the associated risks.

Digital Transformation: Technology has become a huge driver of change and customer interface. This requires AM firms to become reliant on third parties to ensure the availability and integrity of technology supporting investment operations and the client experience.

Optimizing the Vendor Oversight Program: Increased regulator and Board focus on the efficiency, quality, and comprehensiveness of oversight programs. Third-party reporting on internal controls is an essential tool for covering associated risks.

Managing Non-Financial Risks: Asset managers are increasingly relying on third parties to perform tasks that are not specific to financial statement accuracy, but tasks that ensure regulatory compliance, customer experience, and confidentiality.

Protecting Against Cyber Risks: There is an increased focus on addressing cyber risks. AM firms require assurance that third parties are addressing cyber risks proactively.

III. System and Organization Controls (SOC)

SOC suite of services provide independent attestation related to the following subject matter:

SOC for Service Organizations: Providing information that users require to verify internal controls associated with a third-party service provider

- SOC 1 – SOC for Service Organizations: Internal Controls Over Financial Reporting
- SOC 2 – SOC for Service Organizations: Trust Services Criteria
- SOC 3 – SOC for Service Organizations: Trust Services Criteria for General Use Report

SOC for Cybersecurity: Communicating relevant, useful information about the effectiveness of an entity's cybersecurity risk management program – typically performed enterprise-wide

SOC for Supply Chains: Providing risk and control insight into supply chain for customers of manufacturers and distributors

III. System and Organization Controls (SOC)

SOC 1 Type 1

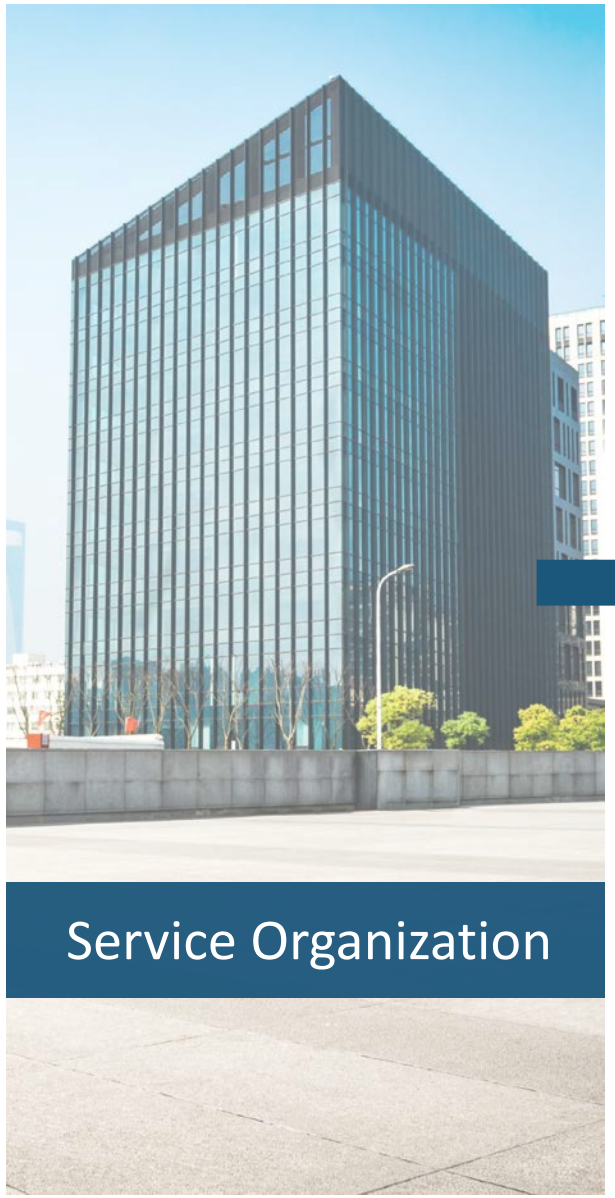
- ✓ Reports on controls placed in operation **at a point in time** *(one date)*
- ✓ Looks at the design of controls – **not** operating effectiveness
- ✓ Considered for information purposes only
- ✓ Not considered of significant use for purposes of reliance by user auditors/organizations
- ✓ Bridge to Type 2 report

Most Reports are Type 2

SOC 1 Type 2

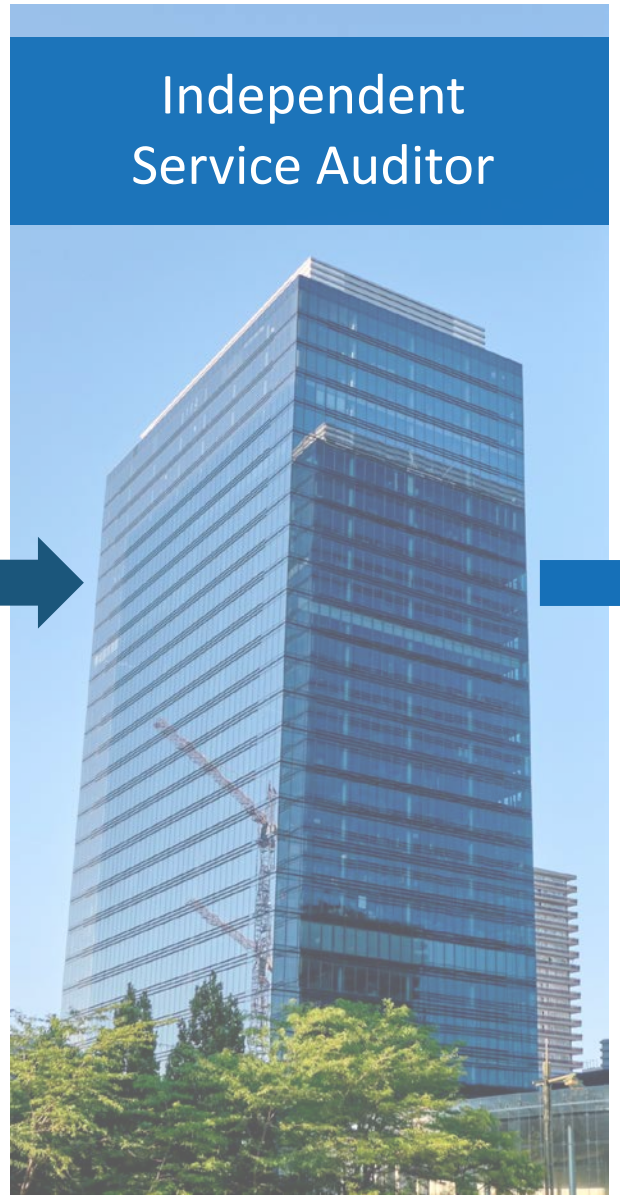
- ✓ Reports on controls placed in operation, and tests of operating effectiveness **for a period of time**
- ✓ Differentiating factor: Includes Tests of **Operating Effectiveness**
- ✓ Identifies instances of non-compliance
- ✓ More emphasis on evidential matter *(more comprehensive than Type 1 – testing of key controls)*
- ✓ Usually a minimum period of 6 months will be reviewed

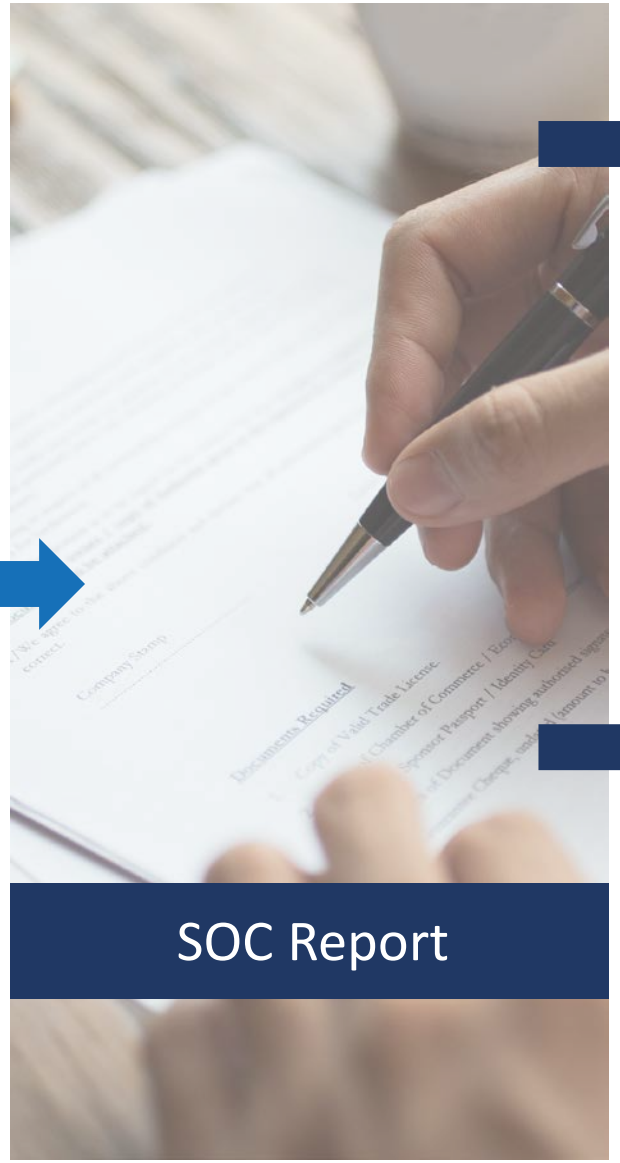
III. SOC for Service Organizations – Key Terminology



Service Organization

Independent Service Auditor





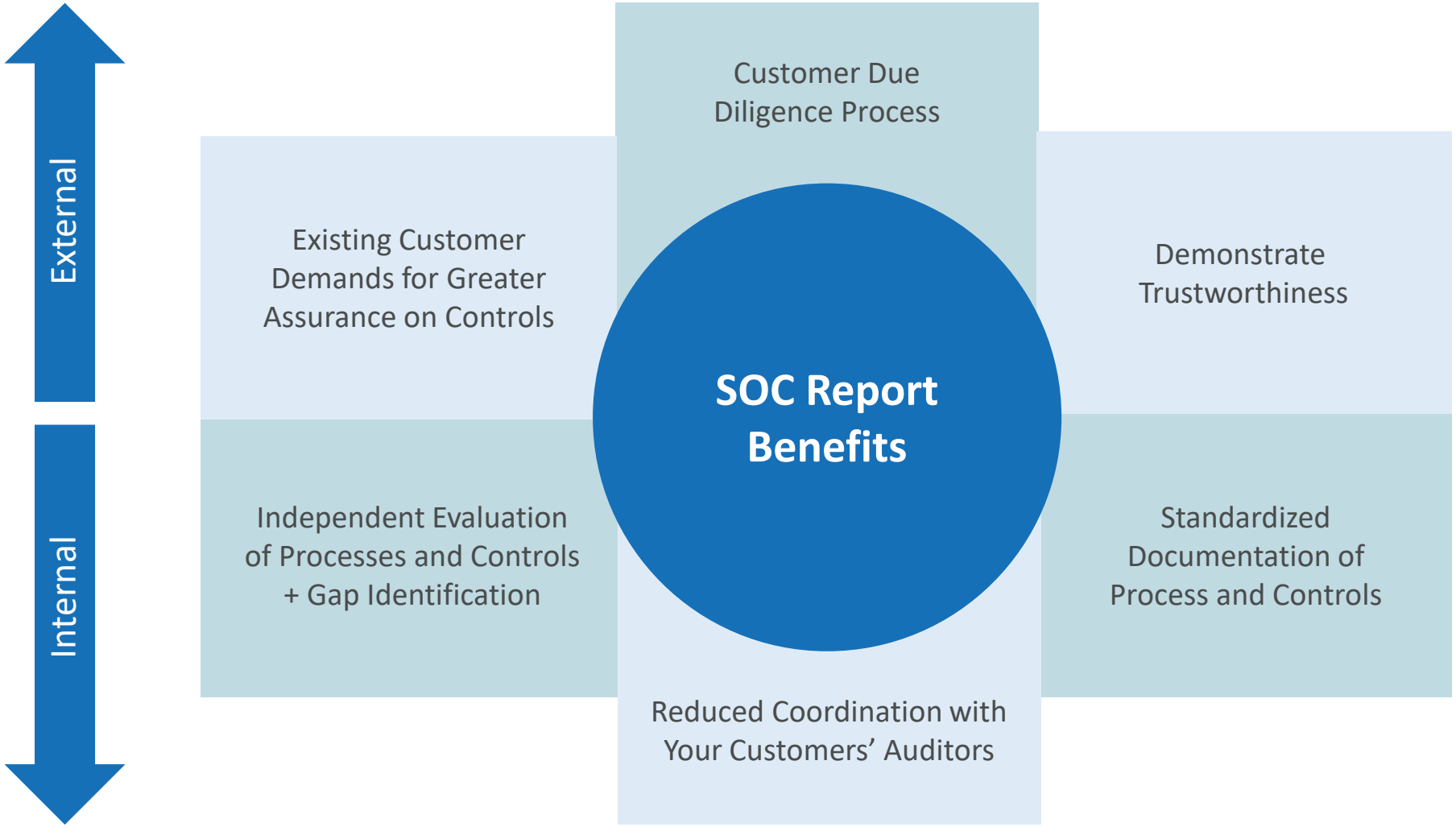
SOC Report

Customer/User Organizations

Complementary User Entity Controls (CUECs)

User Auditors

III. Benefits of Having a SOC Report



III. Typical SOC 1 Report Structure

Section 1: **Auditor's Opinion**

Section 2: **Description of the System**

- Contains management's assertion
- Description of organization and general control environment
- Description of processes being covered by the report

Section 3: **Control Matrix**

- Management's "control objectives" for areas in scope
- Controls supporting the "control objectives"
- Auditor's tests of the controls *(Type 2 only)*
- Results of the auditor's tests *(Type 2 only)*

Section 4: **Other Information Provided by Management**

III. Deviations and Exceptions

INSIGHT

Control	Tests Performed by EY	Results of Tests
Approvals from IT and business management are recorded as part of the change record before changes are implemented to the XYZ application.	For a sample of system changes implemented to the XYZ application, inspected the change record to determine whether approvals from appropriate IT and business management were recorded prior to implementation.	**Deviation noted**: For 2 of 25 changes selected for testing, the approval from IT and business management occurred after implementation as they were not timely notified of the changes. Per inquiry with management, the changes needed to be implemented urgently and were deemed appropriate.

Control Tested

Sample and Nature of Testing

# of Deviations and # Tested

Nature of Deviation

Cause of Deviation

Risk Factors

Considerations impacting the decision to qualify or to not qualify: **Materiality** & **Compensating Controls**

III. Management Response

May be presented in **Section 3** under controls, tests, and results of tests

or in **Section 4**: Other Information Provided by Management *(unaudited)*

- If in Section 3, the auditor is responsible for validating management's response *(part of the audited section of the report)*

Should only contain fact-based information – not forward-looking plans

III. Subservice Organizations

Subservice Organizations: Those vendors who execute controls necessary to achieve one or more of the control objectives (SOC 1) or criterion (SOC 2)

- Monitoring controls over the subservice organization are described by the (primary) service organization

Carve-Out Method

Controls are not included in scope

Complementary Subservice Organization Controls are described by the (primary) service organization

Inclusive Method

Controls are included in scope

Subservice organization provides description and assertion relevant to the services executed

III. Evaluating Reports

User Entity Considerations

- Opinion – Unmodified or Modified?
- Carved-Out Subservice Organizations
- Complementary User Entity Controls
  - Have they been implemented?
- Deviations and Management Responses
- Impact on Company Risk Assessment – What's NOT covered

User Auditor Considerations

- Opinion – Unmodified or Modified?
- Complementary User Entity Controls
  - Can they be tested?
- Deviations and Management Responses
- Impact on Assessment of Audit Risk – Control Risk and Detection Risk
- Period of Coverage
  - Bridge Letters – Purpose and Usability

IV. FICCA Overview – Intermediary Oversight Responsibilities

As mutual fund complexes design their overall financial intermediary oversight program, the **FICCA report can be extremely helpful**, although other elements are important to an effective program

Ideally, an oversight program will involve multiple levels of testing and review. These can – and should – include a thorough inventory of all financial intermediary relationships, as well as a robust **program for payment and invoicing** that clearly **distinguishes different types of payments** *(e.g. shareholder servicing or sub-TA fees)*

Rule 12b-1 fees and revenue sharing agreements with financial intermediaries should also be thoroughly scrubbed to ensure that they correctly reflect the services being performed

FICCA reports are subject to the standard litany of limitations typically found in audit reports, including the **possibility that error or fraud may occur**, but not be detected

IV. FICCA Matrix

The following are the areas contained in the 2014 updated FICCA Matrix:

1) Management Reporting
2) Risk Governance
3) Third-Party Oversight
4) Code of Ethics
5) Information Security Program
6) Anti-Money Laundering
7) Document Retention and Recordkeeping
8) Security Master Set-Up and Maintenance
9) Transaction Processing – Financial and Non-Financial
10) Cash and Share Reconciliations
11) Lost and Missing Security Holders
12) Shareholder Communications
13) Sub-Account Billing, Invoice Processing
14) Fee Calculations
15) Information Technology *(Including Internet and VRU)*
16) Business Continuity / Disaster Recovery
17) Blue Sky Reporting

Note: Intermediaries may not include all areas

IV. FICCA Reporting Overview

As with audit reports generally, **management is required to make certain assertions**, which in this case relate to:

- Its establishment of control objectives
- Whether the controls were suitably designed – as of the specified period end – to provide reasonable assurances that the control objective would be achieved
- Whether the controls were operating effectively, such that the control objectives were met

The auditor in turn expresses an opinion as to **whether management's assertion is fairly stated** based on the specific control objectives.

To arrive at its opinion, the audit firm seeks to obtain an understanding of and evaluate the **suitability of the design and operating effectiveness of the controls**. A summary of the specific controls tested – and the results of those tests – accompanies the FICCA report.

As noted previously, financial intermediaries engage the audit firm, and the auditor report is addressed to management of the intermediary, but will **typically provide that it may be used by the mutual fund complexes**.

IV. Value of FICCA Reporting

- Provides **greater comfort** to those who rely on the compliance controls and processes
- **Reduces oversight performed on existing service providers** *(e.g. Advisor may lessen the oversight of a service provider who utilizes a compliance attestation report)*
- Enables firms to **benefit from industry knowledge of the accounting firm** who conducts attestation *(e.g. We've seen the following controls for this process which you may want to consider implementing)*
- Permits fund Chief Compliance Officer to feel more confident regarding annual **compliance review provided to Board of Directors**
- Provides **greater clarity and transparency** on the processes and controls implemented by providers
- Required by many fund complexes **prior to executing selling agreements**

IV. Lessons Learned – How to Best Prepare for FICCA Engagements

INSIGHT

Common Observations	Example Lessons Learned
A formal risk assessment process to identify key controls and assess the ongoing operating effectiveness may not exist	Identify and prioritize a list of applicable compliance topics and evaluate current risk assessment, policy, procedure, testing, and oversight documentation.
Compliance policies and procedures may either be non-existent, not finalized, or not current	Develop and implement processes to continually update compliance documentation on a reoccurring basis.
A formal annual and ongoing testing program to assess the Compliance Program design and effectiveness may not exist	Implement a formal compliance testing process leveraging key controls identified in risk assessment.
Monitoring and oversight could be enhanced to provide greater transparency of operating effectiveness of compliance policies/procedures and related control activities	Implement a monitoring framework where senior management and Board are proactively notified of material compliance matters.
Roles and responsibilities are not clearly defined	Continually communicate roles and responsibilities to impacted stakeholders and conduct applicable training.
Standardized and formalized escalation protocols may not be clearly defined and documented	Implement a process whereby issues and errors are identified, analyzed, resolved, and communicated to applicable stakeholders.

IV. Recent FICCA Updates by the ICI Working Group – 1 of 2

A key goal of the working group continues to be preserving flexibility for intermediaries when responding to the framework's 14 control Areas of Focus *(Areas 4-17)* where controls are subject to practitioner testing. The 3 information Areas of Focus *(Areas 1-3)* continue to be addressed outside of the practitioner's reports under SSAE-18.

The latest review of the FICCA framework did not alter the list of 17 previously-identified Areas of Focus. However, it did result in a variety of technical enhancements that have been incorporated into the 2020 framework as follows:

- All **terminology was updated to align with AICPA definitions under SSAE-18**, including identification of the applicable attestation standards as well as references to key parties of and reports resulting from various attestation examination engagements used to satisfy the FICCA framework.

- The framework **more clearly separates Areas of Focus into two parts**. The first part includes 14 "control" areas where the service organization *(financial intermediary)* has implemented controls that are tested by the practitioner *(independent auditor)* to determine whether they were suitably designed and are operating effectively to achieve the related control objectives.

- The second part covers 3 "information" areas where the service organization provides background information about its business environment. Information areas do not typically include controls, so practitioner testing is not completed and responses are not considered part of the practitioner's final report.

IV. Recent FICCA Updates by the ICI Working Group – 2 of 2

Subservice organizations *(third-party vendors)* are increasingly important in delivery of services that are relevant to FICCA Areas of Focus. The **"Third-Party Oversight" information Area of Focus reiterates the need, at minimum, to discuss oversight of all relevant subservice organizations** – including identification of any significant situation whereby a subservice organization does not meet expected shareholder servicing standards.

Language was added to the "Consideration for Response" *(formerly "Points to Consider")* in the "Transaction Processing – Financial and Non-Financial" section *(Control Area 9)* to **incorporate compliance with fund money market policies and guidelines under SEC Rule 2a-7**.

The "Sample Management Assertion" section **now includes "Appendix A: Template for Describing Test of Controls and Results"** to organize management's documentation of controls for the 14 control Areas of Focus.

The potential reporting mechanisms within the FICCA framework and related "Mapping Template for Control Reports" were **updated to reflect reports from engagements under AT-C 205** *(formerly "FICCA report")* **or Type 2 SOC 1 under AT-C 320 and the SOC 1 Guide report** *(formerly "AT 801 report")*.

V. NQR – Furthering Audit Report & FICCA Efficiencies

Intermediary INSIGHT

Enables funds to fully realize efficiencies of SSAE 18 & FICCA

- Off-the-shelf solution for analyzing audit reports
- Review all control documentation through FICCA lens
- Direct partnerships with intermediaries
- Forum for peer discussions

Recent FICCA Revisions

Updates focused on alignment with SSAE 18

- FICCA reporting guidance vs. FICCA controls framework
- Importance of subservice organizations (4th parties)
- Revised NQR framework to be instituted October 2020

Service Provider INSIGHT

- Builds on NQR's audit report expertise
- Gap analyses for entire universe of service organizations