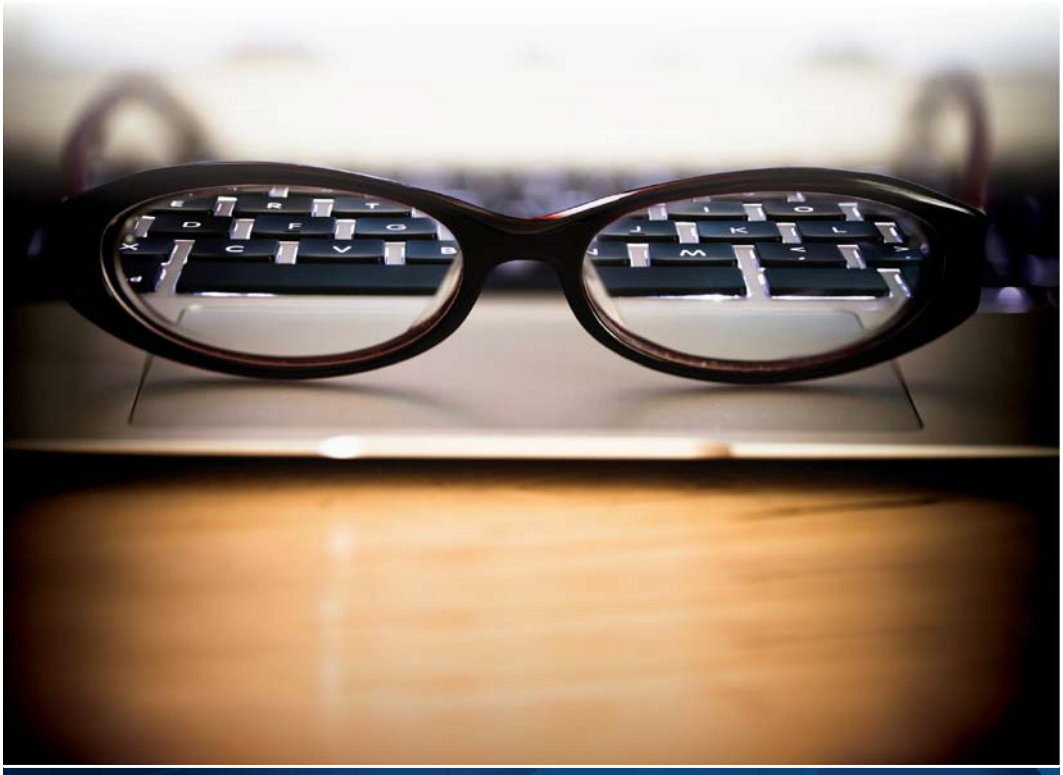
AICPA® Employee Benefit Plan Audit Quality Center

Effective Monitoring of Outsourced Plan Recordkeeping and Reporting Functions



Plan Advisory

The AICPA® EBPAQC is a firm-based, volunteer membership center created with the goal of promoting quality employee benefit plan audits. Center members demonstrate their commitment to ERISA audit quality by joining and agreeing to adhere to the Center's membership requirements. EBPAQC member firms receive valuable ERISA audit and firm best practice tools and resources that are not available from any other source.

Visit the center website at aicpa.org/EBPAQC to see a list of EBPAQC member firms and find other valuable tools prepared for plan sponsors and other stakeholders. For more information, contact the EBPAQC at ebpaqc@aicpa.org.

Table of Contents

Introduction

The AICPA Employee Benefit Plan Audit Quality Center has prepared this advisory to assist you as a plan sponsor, administrator or trustee in understanding the importance and benefits of establishing an effective monitoring program over service organizations that perform recordkeeping and reporting functions for your employee benefit plan. While this advisory specifically addresses service organizations that perform recordkeeping and reporting services, plan sponsors, administrators and trustees should consider how information in the "Selecting and Monitoring Service Organizations" section of this advisory may be useful in monitoring service organizations that perform non-financial functions for the plan.

A plan may use several service organizations such as trustees, custodians, investment managers and recordkeepers to perform various functions on behalf of the plan. The trustee is responsible for the safekeeping of the plan's investments, while the custodian is the party that actually holds the plan's investment securities. Often the custodian also is the trustee. The custodian performs investment functions such as collecting and distributing income and purchasing and selling securities. The plan also may use an investment manager who makes investment decisions and directs the custodian in the purchase and sale of securities. The recordkeeper usually is a third party administrator (TPA), and is responsible for activities such as accounting for participant accounts, valuation of investments, preparation of participant statements and processing distribution checks. If the recordkeeper is the TPA, it also is responsible for plan administration functions such as performing compliance testing, plan design, calculation and allocation of employer contributions, filing the annual Form 5500, *Annual Return/Report of Employee Benefit Plan*, maintaining plan documents and tracking employee eligibility. The recordkeeper is not responsible for the plan's investments.

This advisory discusses:

- Selecting and monitoring service organizations
- The quality of plan accounting information
- Monitoring service organization controls over plan accounting information
- Special considerations for different plan types (defined benefit, defined contribution, and health and welfare plans)

In addition, this advisory includes suggestions for conducting on-site reviews of service organizations and provides examples of controls that help ensure complete and accurate plan accounting information and reporting.

As a generic model, this advisory should be used for reference purposes only. The United States Department of Labor (DOL) publication *Meeting Your Fiduciary Responsibilities* provides an overview of the basic fiduciary responsibilities applicable to retirement plans under the Employee Retirement Income Security Act (ERISA).

The DOL publication is available on DOL's website.

Selecting and Monitoring Service Organizations

Meeting your fiduciary responsibility — As noted in the DOL publication *Meeting Your Fiduciary Responsibilities*, sponsors of employee benefit plans are considered fiduciaries under ERISA. As such, they are subject to certain responsibilities, and with these fiduciary responsibilities comes potential liability: Fiduciaries who do not follow the basic standards of conduct may be personally liable to restore any losses to the plan, or to restore any profits made through improper use of the plan's assets, resulting from their actions.

Your fiduciary responsibilities include plan administration functions such as maintaining the financial books and records of the plan, filing the plan's annual Form 5500 and, in many cases, obtaining a plan financial statement audit. (Federal law generally requires employee benefit plans with 100 or more participants to have an audit as part of their obligation to file an annual return/report.) Plan sponsors and trustees typically use service organizations — such as bank trust departments, data processing service bureaus, insurance companies or other benefits administrators — in some capacity to assist in plan administration: They may outsource investment processing, recordkeeping and/or benefit payments, or claims processing as a way to reduce costs and/or increase efficiencies in administering employee benefit plans.

You should be aware that the hiring of a service organization to perform any or all of the duties noted above is a fiduciary function. In addition, as part of your fiduciary responsibilities, you are required to periodically monitor the service organization to ensure it is properly performing the agreed-upon services. In its publication *Meeting Your Fiduciary Responsibilities*, the DOL points out that one way fiduciaries can demonstrate they have carried out their responsibilities properly is to document the processes used.

How the Use of a Service Organization Affects Your Fiduciary Duty

When a plan sponsor hires one or more service organizations to handle plan administration functions, the agreement typically establishes that the service organization(s) assumes liability for its performance of those functions. For example, if an employer appoints as an investment manager a bank, insurance company or registered investment advisor, the employer is responsible for the selection of the manager, but is not liable for the investment decisions of that manager. However, as noted above, the employer is required to periodically monitor the service organization to ensure it is handling the plan's investments prudently. Prudence focuses on the process for making fiduciary decisions; therefore, it is wise to document decisions and the basis for those decisions, including an employer's selection and monitoring processes.

The Service Organization Selection Process

Selecting Your Service Organization — According to the DOL publication *Meeting Your Fiduciary Responsibilities,* a fiduciary should consider the following when selecting a service organization:

- Information about the firm itself (e.g., financial condition and experience with retirement plans of similar size and complexity)
- The quality of the firm's services (e.g., the identity, experience and qualifications of professionals who will be handling the plan's account; any recent litigation or enforcement action taken against the firm; and the firm's experience or performance record)
- A description of business practices (e.g., how plan assets will be invested if the firm will manage plan investments or how participant investment directions will be handled; the proposed fee structure; and whether the firm has fiduciary liability insurance)

The DOL provides the following tips as a starting point for plan sponsors hiring service organizations:

- Look at a number of organizations, giving each organization the same information, and considering whether the fees are reasonable for the services provided
- Document the hiring process
- Ensure the service organization is clear about the extent of its fiduciary responsibilities
- Obtain a fidelity bond for individuals handling plan funds or other plan property
- Monitor the plan's service organizations

Other important points to consider when hiring a service organization are the ability to access data maintained by the service organization on both a daily and annual basis, and whether the service organization agrees to obtain a Service Organization Controls (SOC 1) report (see the "Monitoring Service Organization Controls Over Plan Reporting" section on page 15 for further discussion of this issue). And finally, you should ensure that a service organization hired to prepare the plan's financial statements will provide you with the support you need to understand those financial statements.

Reviewing and Evaluating the Service Agreement — It is important to ensure that the service agreement between the plan sponsor and the service organization is complete and provides adequate protections for the plan. The service agreement should include predetermined communication and follow-up procedures between the service organization and the plan sponsor in the event of operational issues or other problems identified by the service organization. Certain financial and control measures also should be included in the third-party service organization contract. You should perform a periodic review of follow-up procedures as well as financial and control measures in the contract to ensure they are in place and functioning properly.

This can be achieved easily by requesting that the service organization's periodic reporting cover financial and control measures such as the accuracy and timeliness of recording participant transactions and other measures identified in the contract.

The Service Organization Monitoring Process

Periodic Monitoring of Your Service Organization — As noted above, the plan sponsor or administrator is required to periodically monitor its service organizations to ensure they are properly performing the agreed-upon services. If you use more than one service organization to handle the various plan administration functions, you are responsible for monitoring the activities of each service organization. When monitoring your service organizations, you should:

- Read any reports they provide
- Review the service organization's performance
- Ask about policies and practices
- Check actual fees charged
- Follow up on participant complaints

In addition, *Meeting Your Fiduciary Responsibilities* states that an employer should establish and follow a formal review process at reasonable intervals to decide if it wants to continue using the current service organizations or look for replacements.

Conducting an On-Site Visit at Your Service Organization

On-site visits by you, the plan sponsor, at the service organization are an effective way to review its operations and controls. Such visits may be performed by an individual or a team from Corporate Finance or Human Resources. If this is not practical, phone calls and email contact may be an acceptable alternative. You may decide that spot checks of certain transactions are necessary to determine the quality and accuracy of the service organization's work. This may be especially true when a Type 2 SOC 1 report is not available from the service organization.

You should prepare an agenda that addresses all pertinent issues and areas. While on site, you should tour the facility to get a feel for the operation and atmosphere of the service organization, meet with the employees who perform the work on the account and walk through some of the more critical processes. The meeting or phone call itself should include not only the customer service representative, but the account supervisors and manager, too. Discussion items to consider include:

Monthly/Annual Reports Received From the Service Organization — Reports you should be receiving from the service organization include:

- Contributions by amount and date received from employers or plan participants and date allocated to individual investment options
- Annual participant statement detail (beginning balance, activity detail and ending balance with ending participant balances total tied out to the year-end assets)
- Detail of forfeitures
- Distributions by participant by date
- Asset listing and statement of changes
- Schedule of Assets Held for Investment detail

Conducting an On-Site Visit at Your Service Organization

- List of expenses paid by date with payee
- Trade date versus settlement date reconciliations
- Loan activity/defaulted loans
- Participants with no current address on file
- Party-in-interest/prohibited transactions

Consider the quality of the reports received from the service organization and discuss any related issues. Items to consider include:

- Were reports received in a timely manner?
- Were reports accurate, or did they require amendments?
- Were the reports complete, or were some of them missing information?
- Did the reports contain the information needed to monitor the plan's activity, or is there additional information that would be useful?

New Federal Regulations — You should inquire about any new federal regulations that may affect the plan and how the service organization is implementing them. The service organization should supply a report on the status of any new regulations, including the effective date of the regulation; what changes are necessary to the third-party service organization's systems and reports in order to comply with those regulations; and the third-party service organization's action plan to implement the changes.

Plan Audit and Form 5500 Preparation — You should request that the service organization provide a timeline for the Form 5500 preparation, along with the previous year's timeline. This would be a good time to discuss any problems that arose during the prior year plan audit and

Conducting an On-Site Visit at Your Service Organization

Form 5500 preparation, such as any process improvements and any areas the service organization is aware of that may cause problems in the current year. You also should discuss the audit package that will be sent to the plan auditors, and notify the third-party service organization if there is a change in plan auditors.

Non-Discrimination Testing — You should request that the service organization provide a timeline for non-discrimination testing. At the meeting, you should inquire about whether preliminary testing has been done, and if any issues have been noted as a result. You also should inquire whether the information you provide to the service organization is timely, complete and accurate, and whether the information-transmission process needs to be improved.

Participant Complaints — Logs should be maintained at both the service organization and plan sponsor, with details of participant complaints specific to your plan. Procedures for monitoring and resolving complaints should be reviewed, and you should confirm that all complaints have been or are in the process of being resolved. You also should address any complaints the service organization has received during the year, and ascertain that these complaints are being adequately resolved.

Employee Training/Turnover — The service organization should provide you with an outline of its employee training program and note any changes in the program in the past year. The service organization also should supply a report that details its employee turnover ratio, and the turnover of the staff specifically assigned to the plan's account.

Controls at a Service Organization That Affect the Plan's Financial Reporting/SOC 1 — During the meeting, you should discuss the service organization's controls that are relevant to the plan's financial statements and inquire about any changes implemented during the year. You should

Conducting an On-Site Visit at Your Service Organization

obtain a copy of the service organization's latest SOC 1 report, if applicable, and discuss the findings in the report.

Error Report and Related Corrections — You should ask to see the service organization's error report specific to your plan, which details all errors noted during the period and how they were resolved. This report should include details about the type and date of error, the correction date and any monetary effect. You should review and discuss this report, and inquire how the service organization, if warranted, changed an existing procedure to prevent a similar error from occurring again.

Review Reconciliations — You should ask to review the most current account reconciliations with the service organization, and look to see that the reconciliations are being performed timely and whether reconciling items are being corrected timely. In conjunction with this review, you should ensure that amounts deposited were allocated. You also should discuss the nature of any old reconciling items and the reasons they have not been corrected.

Other Requests — You should prepare a list of reports and information you would like to receive that are not currently available. This list should be discussed with the service organization during the meeting.

Benefits of an Effective Monitoring Program — An effective monitoring program helps ensure you are meeting your fiduciary responsibilities. It also helps the plan sponsor gauge the quality of services performed by the service organization and provide valuable information regarding the service organization's controls and their effectiveness. It also can be helpful in identifying potential cost savings, areas for improved efficiencies and opportunities to improve participant satisfaction. And, as discussed below, it can result in cost savings in connection with the annual plan audit.

Corresponding With Your Service Organization — You should regularly correspond with your service organizations. Depending on the size and complexity of the plan(s) involved, it may be appropriate to contact the service organization as often as quarterly, but no less frequently than annually. Face-to-face meetings can take place either at your place of business or the service organization's location. See sidebar on pages 8 through 11 for suggestions for conducting an on-site visit at your service organization, including discussion topics.

Performing an Annual Reassessment of the Effectiveness of the Service Organization Relationship — Evaluate the reasonableness of fees charged for the services, the quality of the services provided, the quality of the service organization's operations and the availability of a SOC 1 report.

Monitoring Participant Communications and the Participant Complaint Process — Participants should have a formalized process to submit questions or file complaints, and should receive periodic statements of their account balances and/or confirmations of their transactions. This will help ensure any errors in participant accounts are identified on a timely basis. You should maintain a complaint log and ensure all questions/complaints are followed up on and resolved in a timely manner.

Quality of Plan Accounting Information

The plan sponsor may hire a service organization to provide plan accounting services, including preparing participant account balance information, investment reports and tax reports; preparing monthly or periodic accounting reports used in preparing the plan's financial statements; and preparing the plan's Form 5500. It is important to note that the plan administrator (who may be the plan sponsor) remains primarily responsible for filing complete and accurate plan financial statements and Form 5500 information with the DOL. Inaccurate or incomplete filings can result in the Form 5500 being rejected by the DOL, with significant penalties assessed on the plan administrator. Therefore, *it is important that you ensure you are receiving reliable and accurate information from the service organization.*

Understanding the Accounting Information — As a plan sponsor, you are responsible for the plan's financial reporting; therefore, you need to be familiar with the accounting framework used to prepare the plan's financial statements (modified cash or accrual method using U.S. generally accepted accounting principles as promulgated by the Financial Accounting Standards Board (FASB) (GAAP) used by the service organization.) If the plan issues financial statements on the accrual basis, you should consider whether adjustments to the information provided by your service organization may be necessary to prepare the plan's financial statements consistent with GAAP. For example, the service organization may net items of income and expense that are required to be reported separately; exclude certain plan assets and liabilities; or inconsistently or incorrectly group expenses. You may want to consult with the plan's audit firm on the appropriate accounting and reporting requirements. In addition, you should check to ensure that the service organization reports include adequate information to meet other DOL reporting requirements.

Reading the Service Organization Reports — A periodic review of the plan reports prepared by the service organization for consistency, completeness and reasonableness can be an effective step in ensuring the

accuracy of the accounting information provided by the service organization. A key component of this review is the consistency of the information in the reports pertaining to the plan and its operations. Specifically, you should:

- Compare the information in the report with that in prior-period reports. If significant differences exist, investigate the reasons for those differences
- Consider whether the report reflects all relevant information about the plan and its transactions. Also ensure that the report provides you with adequate information to carry out your fiduciary duties as plan sponsor
- Review the report in relation to what you know about the plan's structure, participants and operations, to determine if information and amounts reported make sense and are reasonable

Checking Account Reconciliations — Another valuable step is a review of account reconciliations performed, and a comparison of specific amounts in the reports with the client data used in the reconciliations (e.g., the amount of contributions made by the plan sponsor and/or plan participants). You also should ensure that reconciling items are specifically identified and that they clear in a timely manner.

Reviewing for Overall Reasonableness — Analytical review procedures performed on account balances and activity is an effective way to determine that the information being reported is reasonable. For example:

- Compare the plan's total return on investments to published sources for the total return of the underlying investments
- Compare expected participant head count (prior year head count adjusted for expected changes during the year) to actual participation levels in the plan at year-end
- Review distribution listings for unusual items (for example, payments to people who have not terminated or have been difficult to locate in the past or lump-sum payments from a defined benefit pension plan that seem high)

Monitoring Service Organization Controls Over Plan Accounting Information

Strong Controls Are Essential — Strong controls at the service organization are essential for ensuring plan information is complete and accurate; they are vital to the plan's financial reporting process. Another key step in effectively monitoring the service organization is to understand the quality and effectiveness of the processes, procedures and controls used to produce the plan's accounting information. (These controls will vary, depending on the services you hire the service organization to provide.) In evaluating the service organization, you should determine whether:

- Participant enrollments, cash receipts, distributions of plan assets, exchanges of plan assets among investment options and changes to non-financial account information are processed completely, accurately and in a timely manner, according to instructions from plan sponsors and participants
- Dividends are timely and accurately recorded
- Transactions for each investment option are applied with the correct market prices; ending investment balances are applied with the correct market prices; and the resulting net appreciation/depreciation is reflected in participant accounts
- Plan assets are safeguarded from loss or misappropriation
- Participant access to data via voice or Internet is properly authorized and secured

- Participant transaction confirmations, account statements and plan level periodic reports are accurate, complete, timely and made available to participants and/or plan sponsors without intervention by service organization employees responsible for processing those transactions

- Annual plan-level financial statements are complete, accurate and mailed on a timely basis to the plan sponsor

- Year-end compliance tests are complete and accurate

- Changes to existing systems software and implementation of new systems software are tested, approved and documented prior to promoting to production

- Access to service organization physical facilities and software programs and data is limited to authorized individuals and controls exist to protect them

- New plans, mergers and transfers are established in accordance with the plan document, and participant, financial and demographic data are accurately recorded

AICPA's Audit and Accounting Guide, *Employee Benefit Plans* includes suggestions regarding the use of SOC 1 reports and examples of controls for employee benefit plans in the areas of investments; contributions received and related receivables; participant loans; benefit payment claims and distributions; participant data and plan obligations; administrative expenses; reporting; and general computer controls (in-house system or service organization); and user controls when a service organization is utilized.

How a SOC 1 Report Can Help — An effective approach to help you, the plan sponsor, understand and monitor the quality and effectiveness of the service organization's processes and controls is to request a report on controls at the service organization that affect the data and other information provided to the plan and included in the plan's financial statements. Such reports commonly are referred to as service organization controls (SOC) 1 reports and are provided by a CPA who performs an examination of controls

at the service organization under AICPA Professional Standards (these reports previously were referred to as SAS 70 reports). Concern over the quality of accounting information, increased reliance on outsourcing and increased use of technology in plan administration services has resulted in greater demand for SOC 1 reports. A type 1 SOC 1 report includes a detailed description prepared by the service organization's management of the service organization's system and controls that may be relevant to the plan's financial statements, and a CPA's independent assessment of whether the description is fairly stated and the controls are suitably designed. A type 2 SOC 1 report contains the same information as a type 1 SOC 1 report but also includes a description of the CPA's tests of controls and results of those tests. As discussed below, a type 2 SOC 1 report will tell you if the service organization's controls are operating effectively.

SOC 1 reports can be extremely important to you in fulfilling your fiduciary duty to monitor your service organization; as such, you should obtain and read a copy each year. After reviewing the SOC 1 report, you may wish to document your assessment of the service organization's controls and any responses to testing errors. Such documentation provides support for the fiduciary due diligence you perform in that area.

Service organizations are not required to furnish SOC 1 reports. However, because these reports are so important to you and the plan auditor (see the "Not Having a SOC 1 Report May Have a Significant Negative Effect on You as Plan Sponsor" and "Consider the Potential for Cost Savings" sections, below), it is in your best interest to make certain when you hire or retain the service organization that the service organization agrees to obtain a SOC 1 report. In addition, you may wish to meet with your plan auditors to assist you in determining which controls are important to the financial reporting process.

Not Having a SOC 1 Report May Have a Significant Negative Effect on You as a Plan Sponsor — If a SOC 1 report is not available from the service organization, then it will be more difficult for you — as well as the independent auditor — to ascertain whether the controls at the service organization are suitably designed and operating effectively. In that case, you and the auditor likely would need to perform other procedures

to assess the service organization's control environment. These procedures may include reading the user manuals or other systems documentation about the services provided; reading the reports of the internal auditors or regulatory authorities on the service organization's controls; and making inquiries of personnel at the service organization. It may be necessary for you and the auditor to perform a site visit to the service organization at additional expense to you. You also should be aware that if no SOC 1 report is available, and the auditor is unable to perform procedures at the service organization to satisfy his or her objectives, then the auditor must disclaim an opinion or issue a modified opinion on the plan's financial statements. If either of those types of reports is issued, it will be rejected by the DOL, and you may be subjected to monetary penalties.

Consider the Potential for Cost Savings — Another benefit to using a service organization that obtains a SOC 1 report is the potential cost savings on audit fees. SOC 1 reports (especially type 2 SOC 1 reports) may save plan auditors time. You should be aware, however, that not all SOC 1 reports will enable an auditor to reduce the amount of work performed with regard to controls at the service organization. Independent auditors will not be able to use a SOC 1 report that is issued by a party other than a CPA or a CPA firm. In addition, the auditor may not be able to use a SOC 1 report that lacks sufficient detail; does not include information about transactions, control objectives or individual controls relative to the plan; or does not coincide with the plan's reporting period.

Understand the Different Types of SOC 1 Reports — There are two types of SOC 1 reports. It is important that you understand whether a type 1 SOC 1 report or a type 2 SOC 1 report was issued, and what it means.

Comparison Of Type 1 and Type 2 SOC 1 Reports	
Type 1 Report	**Type 2 Report**
Service organization's auditor expresses an opinion on whether, in all material respects, based on the criteria: 1. The service organization's description of its system fairly presents the service organization's system that was designed and implemented as of a specified date.	Service organization's auditor expresses an opinion on whether, in all material respects, based on the criteria: 1. The service organization's description of its system fairly presents the service organization's system that was designed and implemented throughout a specified period.
2. The controls related to the control objectives stated in the service organization's description were suitably designed to provide reasonable assurance that those control objectives would be achieved if the controls operated effectively as of a specified date. **Note:** It does not include an opinion about the operating effectiveness of the service organization's controls.	2. The controls related to the control objectives stated in the service organization's description were suitably designed to provide reasonable assurance that those control objectives would be achieved if the controls operated effectively throughout the specified period.

Comparison Of Type 1 and Type 2 SOC 1 Reports (Cont'd)	
	3. The service organization controls that were tested, which were those necessary to provide reasonable assurance that the control objectives stated in the service organization's description were achieved, operated effectively throughout the specified period. **Note:** Because this report addresses the effectiveness of the service organization's controls, it is the most useful for both audit and quality monitoring purposes.

Familiarize Yourself With the Contents of a SOC 1 Report — A SOC 1 report includes management's description of: The types of services provided and the classes of transactions processed; procedures by which services are provided; related accounting records and supporting information; how the service organization captures other significant events and conditions other than transactions; processes used to prepare reports and other information; control objectives and controls designed to achieve them; and other aspects such as the control environment, risk assessment process, information and communication systems and changes to such systems.

Key elements you might see in the description include:

- Overview of the service organization, organizational structure and control environment, including commitment to governance, business ethics and compliance management

- Description of the service organization's plan services IT environment and processing systems
- Description of general IT controls, including business systems, IT operations, information security management and IT control environment
- Description of business process for key areas, including contribution and loan repayments, withdrawals and loans, contribution allocation changes, dividend processing, pricing, investment return, plan financial reporting and compliance testing

A SOC 1 report also will include a written assertion by management of the service organization about whether its description of the service organization's system fairly presents the service organization's system and whether the controls related to the control objectives stated in the description were suitably designed to achieve those control objectives. In a type 1 report, this assertion will be as of a specified date; in a type 2 report, it will cover a specified period. In addition, in a type 2 report, management's written assertion will address whether the controls related to the control objectives stated in management's description of the service organization's system operated effectively throughout the specified period to achieve those control objectives.

Finally, a SOC 1 report will include the service auditor's report. The table on page 19 and 20 describes and compares the type 1 and type 2 SOC 1 reports.

Note the Documented Controls and Scope of Testing Performed — The service organization's description of its system is an integral part of a SOC 1 report, and will help you determine if the controls are adequate to ensure complete and accurate financial reporting. Also of particular concern is the scope of the auditor's work described in the report. This section should be carefully reviewed to ensure it covers all significant transactions, processes or IT applications that affect the plan's financial statements.

Look for Any Carve-Outs — In some cases, the service organization may use another service organization *(subservice organization)* to process certain transactions or perform certain functions. In those cases, management's description of the service organization's system will either include the relevant information related to the subservice organization or will "carve out" those areas from its description. For example, a service organization may use a data processing subservice organization but still maintain responsibility for restricting logical access to the system to properly authorized individuals. In such cases, management may identify the nature of the services performed by the subservice organization and exclude from the description — and from the scope of the service auditor's engagement — the subservice organization's relevant control objectives and related controls. In such cases, the service auditor's engagement will not extend to the subservice organization. AICPA Professional Standards provide the following example of language that might be included in a service auditor's report to indicate that the report does not cover a carved-out function:

> XYZ Service Organization uses a computer processing service organization for all of its computerized application processing. The description on pages [bb–cc] includes only the controls and related control objectives of XYZ Service Organization and excludes the control objectives and related controls of the computer processing service organization. Our examination did not extend to controls of the computer processing service organization.

Depending on the significance of the carved-out areas, you may need to obtain a SOC 1 report from the other service organization.

A type 1 SOC 1 report may be as of a date other than the plan's year-end, and a type 2 SOC 1 report may cover a different reporting period than the plan's fiscal year. You should consider these timing issues when evaluating the usefulness of a SOC 1 report for your monitoring activities. If the period not covered by the report is significant, you should consider reviewing documentation and correspondence issued by the service organization regarding changes to application systems and controls. In addition, you should make inquiries of service organization personnel about changes to the application system or related controls outside the reporting period, changes in the reliability of the processing of financial information, and whether the

service auditor could apply agreed-upon procedures to supplement the SOC 1 report.

Evaluate Any Deviations Identified — It is important that you understand what controls should be in place, and whether they are operating effectively. When the service organization's SOC 1 report identifies deviations, you should consider the effects of the findings on plan operations. When evaluating the significance of deviations, you should make sure to fully understand the situation noted by the service auditor and its effect on the organization's controls. If there are areas where controls are inadequate, you should determine what complementary controls at the plan are required. Such controls are referred to in SOC 1 reports as *user entity controls*.

Complementary User Entity Controls — If effective controls are not in place at the plan, the service organization's controls may not compensate for such weaknesses. In many cases, the SOC 1 report will include in management's description of its system the complementary user entity controls for which the plan (user entity) is responsible. For example, with respect to new participant accounts and changes to participant data, the report might state that the plan sponsor is responsible for:

- Sending participant data to the service organization in a specified format
- Determining eligibility
- Establishing plan guidelines for authorizing the service organization to process new participants and changes to participant data
- Establishing controls to ensure that new participant data and changes to participant data are communicated timely

Turn the page for a detailed list of 13 example complementary user entity controls.

Complementary User Entity Controls

1. The plan sponsor is responsible for establishing controls to determine employee eligibility to participate in the plan, and to allow those who are eligible the opportunity to participate.
2. Each plan sponsor is responsible for establishing controls to ensure employee payroll information sent to the service organization for contributions (employer and employee) and loan repayments is accurate, complete and received by the service organization on a timely basis.
3. Each plan sponsor should establish controls to ensure that participant information and requests submitted by the plan sponsor are accurate, complete, properly authorized and in accordance with the plan requirements and provisions. Participant forms include, but are not limited to, enrollments, loans, exchanges, contribution allocation changes, distributions and demographic changes, which are submitted manually and/or electronically.
4. The plan sponsor is responsible for establishing controls for determining when a participant loan is in default.
5. The plan sponsor is responsible for establishing controls relating to the timely review of plan reports — including annual plan financial statements, distribution reports, conversion reports, participant records and statements provided by the service organization — and notifying the service organization of any discrepancies in a timely manner.
6. To the extent that a plan sponsor has access to the service organization's terminals and systems, the plan sponsor is responsible for establishing and maintaining adequate controls over physical and logical access at the plan sponsor locations.
7. To the extent that a plan sponsor has direct access to the service organization's applications, the plan sponsor is responsible for establishing controls to ensure timely notification to the service organization of personnel changes affecting user access.

Complementary User Entity Controls (Cont'd)

8. To the extent that a plan sponsor has online access to the service organization, the plan sponsor is responsible for establishing controls to properly administer user identifications and passwords, and to monitor user activity.
9. The plan sponsor is responsible for implementing procedures to ensure the service organization receives notification of all transactions.
10. The plan sponsor is responsible for notifying the service organization, in a timely manner, of changes in individuals authorized to instruct the service organization on the plan sponsor's behalf.
11. Plan sponsors are responsible for establishing controls to communicate plan amendments and changes that affect plan recordkeeping in a timely manner.
12. The plan sponsor is responsible for notifying the service organization when and how to allocate forfeitures.
13. For plans that use a Form 5500 preparation service, the plan sponsor is responsible for providing accurate and timely information to the service organization for the preparation of Form 5500. The plan sponsor is responsible for filing Form 5500 with the IRS by the specified due date.

The AICPA's Audit and Accounting Guide, *Employee Benefit Plans* includes examples of selected complementary user entity controls for employee benefit plans in the areas of investments; contributions received and related receivables; participant loans; benefit payment claims and distributions; participant data and plan obligations; administrative expenses; reporting; and general computer controls.

Special Considerations for Different Plan Types

Defined Benefit Pension Plans

Defined benefit pension plans often invest in a full array of marketable and non-marketable securities. Typically, a trustee and/or custodian hold investments and execute investment transactions on behalf of the plan and prepare the year-end statements used as the basis for the financial statements.

The investment balances and activity in the underlying reports provided by the trustee/custodian are used as a basis for preparing the financial statements and investment disclosures; thus, you may wish to review that information to determine its accuracy. The review should consider:

- Whether the investments are properly classified (e.g., investments in bank collective trust funds or limited partnerships classified as registered investment companies)

- Whether derivative investments are recorded on the trustee/custodian statement. Such investments sometimes are recorded off-line or reported at zero on the schedule of investments provided by the trustee/custodian, requiring additional detail in order to compile financial statement information

You also should consider the importance of gaining an understanding of the accounting and reporting by the trustee/custodian for non-marketable investments to ensure they are reported in accordance with generally accepted accounting principles. Fair value adjustments should be made to the trustee/custodian statements as part of the financial statement compilation process performed by the plan sponsor at year-end.

Defined Contribution Pension Plans

Many 401(k) plans outsource the administration of the plan to a service organization under a full-service agreement. In these circumstances,

participant transactions are initiated directly with a third-party recordkeeper, which interfaces directly with a third-party payroll processor for recording contributions. The recordkeeper prepares year-end financial reports, including the DOL's Form 5500.

Service organizations market such arrangements to plan sponsors as a way to offer 401(k) benefits with minimal involvement from the plan sponsor. As noted above, the plan sponsor still has a fiduciary responsibility to periodically monitor the activities of the service organization. The suggestions in this document can help plan management ensure that proper monitoring of the service organization is performed.

Health and Welfare Benefit Pension Plans

For various reasons — such as convenience, expertise and confidentiality — health and welfare benefit plan sponsors often engage one or more third parties to process claims (e.g., health, dental and disability benefits). In such cases, plan sponsors do not maintain independent records of the claims paid. Claims payments generally are the most significant element of health and welfare plan financial statements, and often are significant to plan-sponsor operations as well.

As noted above, you have a fiduciary responsibility to periodically monitor the activities of the service organization. In addition to reading the SOC 1 report, if available, examples of effective monitoring controls include:

- Review of periodic (e.g., monthly or weekly) claim information at a reasonably detailed level of disaggregation (number of claims, type of service, number of employees receiving benefits, dollar amount of claim, deductible applied, and reasonable and customary allowances applied) that allows the sponsor to conclude that claims paid are for covered services and amounts paid are consistent with plan provisions

- Review of census information from the claims processor in sufficient detail to conclude that only eligible plan participants are receiving benefits

- Performance of analytical procedures using disaggregated information (e.g., comparisons of average claim per participant to the expected number of claimants taking into account plan amendments, individual large claims, stop loss insurance coverage or the health care cost trend rate increase). The claims processor often prepares quarterly reports, which include head count and claim information that can be used to assist in analytics

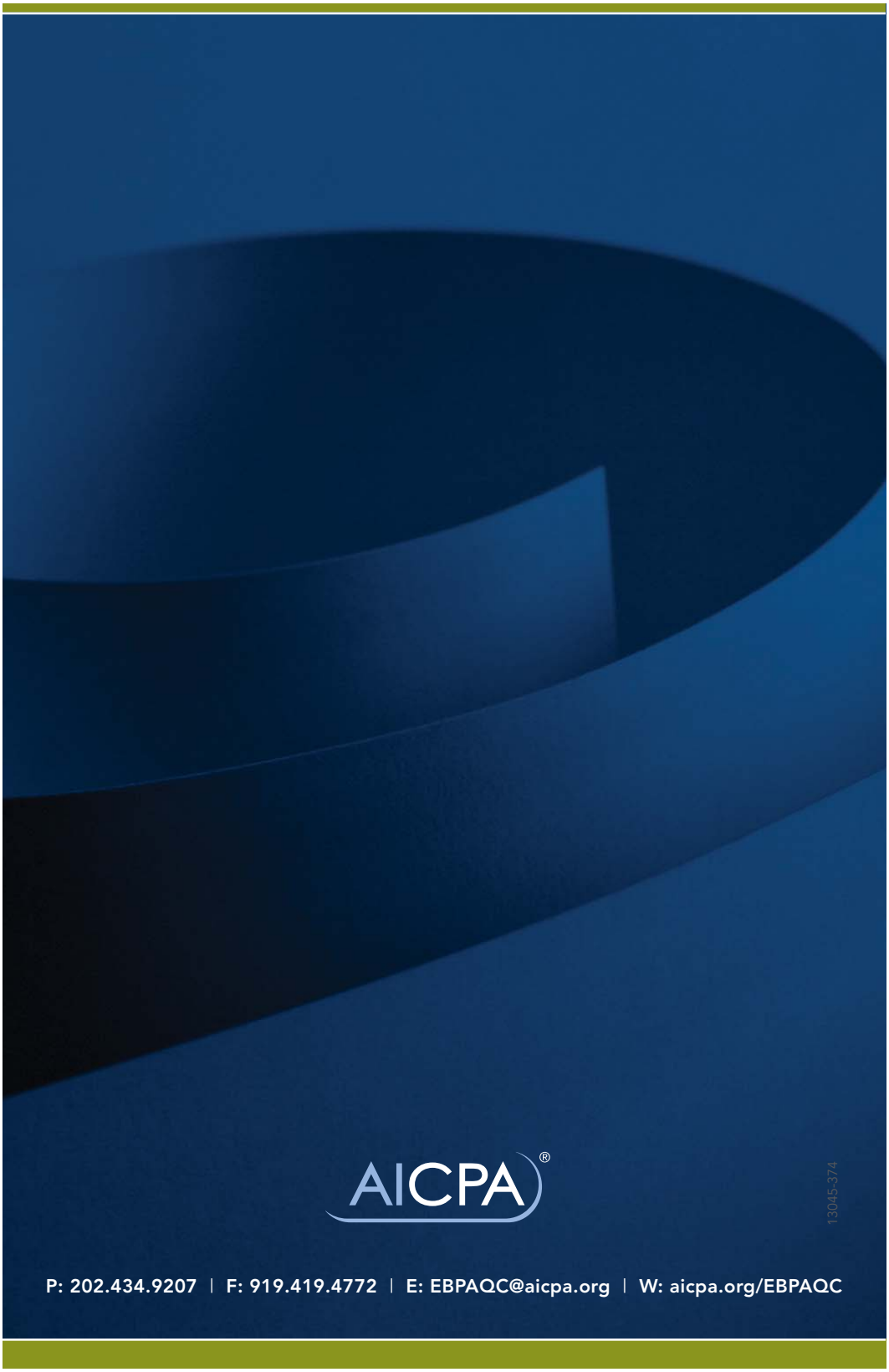
For more information about the AICPA Employee Benefit Plan Audit Quality Center and employee benefit plan audits, visit the center's website at aicpa.org/EBPAQC.

Additional Resources

AICPA Practice Aid *Using an SSAE No. 16 Service Auditor's Report (SOC 1 Report) in Audits of Employee Benefit Plans* may serve as a useful tool as you carry out your fiduciary responsibilities in monitoring the activities of service organizations. This publication is available on the AICPA's website. You also may wish to ask your plan auditor for assistance in understanding the SOC 1 report.

AICPA Audit and Accounting Guide, *Employee Benefit Plans* includes examples of selected complementary user-entity controls at your service organization and for your employee benefit plans. The guide is available on the AICPA's website.

Meeting Your Fiduciary Responsibilities, a United States Department of Labor (DOL) publication, provides an overview of the basic fiduciary responsibilities applicable to retirement plans under the Employee Retirement Income Security Act (ERISA). The publication is available on DOL's website.


AICPA®
13045-374
P: 202.434.9207 | F: 919.419.4772 | E: EBPAQC@aicpa.org | W: aicpa.org/EBPAQC