ERISA Roundup

A quarterly recap of recent publications from BDO's ERISA Center of Excellence

Q3 2025

BDO

A Note from BDO's ERISA Practice Leaders

Fall is here, the leaves have changed, and things have finally started to slow down after the hustle of plan audits and Form 5500 filings. If you've been putting off any retirement plan tasks, now's a great time to check them off your list.

In this edition of our ERISA Roundup, you'll find information on forfeitures, explore more about pooled employed plans, and make sure your plan is in compliance with the upcoming SECURE 2.0 plan amendment deadlines.

Staying current on ERISA topics is simplified with BDO: Follow along with our regular insights at our **BDO ERISA Center of Excellence**. We welcome your feedback on our content at **BDOTalksERISA@BDO.com**.

BDO's ERISA Center of Excellence is your source for insights on emerging regulations, industry trends, current topics, and more. Visit us at www.bdo.com/erisa or follow along on X: @BDO_USA and #BDOERISA.

MARY ESPINOSA
Assurance Principal
Employee Benefit Plans

ERIN BREIT
Assurance Principal
Employee Benefit Plans

NICOLE PARNELL
Tax Principal
Global Employer Services
Retirement Plan Services Leader

LUANNE MACNICOL
Assurance Principal
Employee Benefit Plans

JESSICA FRIEDLY
Assurance Principal
Employee Benefit Plans

MICHAEL BELONIO
Assurance Principal
Employee Benefit Plans

KAROLYN LADAS
Assurance Principal
Employee Benefit Plans

In this Issue

2025 Deadlines and Important Dates

Sponsors of defined benefit and defined contribution retirement plans should keep the following deadlines and other important dates in mind as they work toward ensuring compliance for their plans in 2024. Dates assume a calendar year plan. Some deadlines may not apply, or dates may shift based on the plan sponsor's fiscal year. For additional support, please contact your BDO representative.

DOWNLOAD THE FULL CALENDAR YEAR ▶

OCTOBER

- **3** / **Action:** Distribute annual notices to participants no earlier than October 3 and no later than Dec 2, including notices for: 2026 401(k) Plan Safe Harbor Match, Automatic Contribution Arrangement Safe Harbor, Automatic Enrollment and Qualified Default Investment Alternatives (QDIA).
- **15** / **Fund:** Possible third quarter 2025 contribution due for defined benefit pension plans by October 15.
- **15** / **Action:** October 15 is the extended deadline for filing IRS Form 5500 and IRS Form 8955-SSA.
- **15** / **Action:** October 15 is the extended deadline for filing individual and C-Corp tax returns.
- **15** / **Action:** If an extension was filed, October 15 is the deadline to fund defined contribution employer contributions for C-Corporations and Sole Proprietors.
- **15** / **Action:** October 15 to open a Simplified Employee Pension (SEP) plan for extended tax filers.
- **15** / **Action:** Send annual funding notice to participants of single- and multi-employer defined benefit plans with 100 or fewer participants by October 15.
- **15** / **Action:** October 15 , defined benefit plan PBGC Premium filings and payments due.
- **31** / **Action:** Single-employer defined benefit plans that are less than 60% funded or are 80% funded and have benefit restrictions triggered must inform participants by October 31 or 30 days after the benefit restriction applies.

DECEMBER

- **1** / **Action:** Distribute annual participant notices no later than December 2 for the 2026 upcoming calendar year plan year. These include notices for: 401(k) Plan Safe Harbor Match, Automatic Contribution Arrangement Safe Harbor, Automatic Enrollment and Qualified Default Investment Alternatives (QDIA).
- **15** / **Action:** December 15 is the extended deadline to distribute Summary Annual Report (SAR) when the Form 5500 was filed on October 15.
- **31** / **Action:** December 31 is the final deadline to process corrective distributions for failed ADP/ACP testing; a 10% excise tax may apply.
- **31** / **Action:** Ongoing required minimum distributions (RMDs) for 5% business owners and terminated participants must be completed by December 31.
- **31** / **Action:** Amendments to change traditional 401(k) to safe harbor design, remove safe harbor feature or change certain discretionary modifications must be completed by December 31. Amendments to change to safe harbor nonelective design must be completed by Dec 1 of given plan year for 3% or by Dec 31 of the following year for 4% contribution level.
- **31** / **Action:** Plan sponsors must amend plan documents by December 31 for any discretionary changes made during the year.

UPCOMING WEBINAR

Navigating ERISA Compliance in 2025

TUESDAY, NOVEMBER 18, 2025

1:00 to 2:00 PM ET

CPE Credit 1.0

Presented by:

LINDA BAKER
Senior Manager
Global Employer Services
Retirement Plan Services
BDO USA

JENNIFER JACKSON
Senior Manager
Global Employer Services
Retirement Plan Services
BDO USA

NICOLE PARNELL
Principal
Global Employer Services
Retirement Plan Services
BDOUSA

As regulatory complexity continues to evolve, retirement plan sponsors and fiduciaries must stay ahead of critical compliance deadlines and procedural updates. Join us for a timely and informative webinar that breaks down the latest guidance and practical implications of key ERISA developments.

We'll explore:

- **New Guidance on Roth Catch-Up Contributions**: Understand the new mandatory Roth treatment for catch-up contributions by high earners starting in 2026. Learn how plan sponsors can prepare for implementation, including payroll integration and participant communications.
- **DOL Delinquent Filer Voluntary Compliance Program (DFVCP):** Review recent changes to the DOL's on-line DFVCP platform for correcting late Form 5500 filings. Discover how the DFVCP offers relief and what changes may impact your filing strategy.
- **Plan Amendment Deadlines for Changes in the Law Since 2019:** Get clarity on mandatory amendment timelines and best practices for coordinating with service providers, for all changes in the law affecting tax-qualified retirement plans since 2019. We'll share actionable steps to streamline your amendment process and avoid last-minute compliance risks.
- **Record Retention Rule Reminders:** Revisit ERISA's recordkeeping requirements and learn how to align your retention policies with current enforcement expectations. We'll highlight common pitfalls and how to avoid them.

Key Takeaways Include:

- Review mandatory Roth treatment for catch-up contributions by high earners starting in 2026. List what service providers and plan sponsors must do now to prepare for implementation and identify best practices for ongoing compliance.
- Identify how to leverage the DOL's (DFVCP) to correct late Form 5500 filings and avoid escalating penalties. We'll share recent enforcement trends and practical tips for timely compliance.
- Review the IRS-mandated deadlines for plan amendments for changes in law since 2019 including the CARES Act, SECURE 1.0 Act and SECURE 2.0 Act. Discover how to coordinate with third-party vendors and internal stakeholders to ensure timely adoption and avoid disqualification risks.

REGISTER FOR WEBCAST ▶

The Story of PEPs: Revisiting Pooled Employer Plans in 2025

The rationale underpinning PEPs is that companies can benefit from their pooled buying power to lower administrative and investment costs. Employers can also transfer some fiduciary liabilities and administrative burdens to third-party pooled plan providers.

As the ERISA-named fiduciary for the plan, the Pooled Plan Provider (PPP) must operate the PEP in the best interests of the participants. Responsibilities include assuming administrative duties, filing the annual Form 5500 on behalf of the participating employers, and responding to audits and investigations conducted by the DOL and/or Internal Revenue Service (IRS). Additionally, the pooled plan provider must be insured. Depending on how the plan is designed, the PPP may also serve in the role of 3(38) investment fiduciary, allowing it to develop the PEP investment policy, as well as select, monitor, and replace the PEP investment options.

Participating employers are responsible for selecting an initial provider that is qualified to administer the plan, as well as for continuing oversight and monitoring of the PEP and its performance. It is critical to the plan's operations that participating employers provide accurate data to the PPP, including new hire dates, deferral amounts, loan repayments, and more. Remitting contributions to the PEP on time and providing complete and accurate contribution data are also responsibilities that fall to the employers.

MAINTAINING REPUTATION AND CULTURE

The SECURE Act includes provisions aimed at increasing access to workplace retirement plans through the creation of PEPs. Specifically, the law seeks to address some of the restrictions and perceived drawbacks of MEPs, while creating new benefits for PEP participants.

In addition to reducing administrative and fiduciary burdens, PEPs offer several potential benefits, including:

- **Tax Credits:** Eligible employers can receive up to $5,000 in tax credits to offset startup costs and an additional $500 tax credit annually for the first three years for automatically enrolling participants in the plan.
- **Bad Apple Rule:** The SECURE Act also eliminated what many employers considered an obstacle to joining a MEP: the "one bad apple" rule. Historically, the entire MEP could be disqualified if a single participating employer failed one of the many plan qualification rules. But with a PEP, the failure of one employer to meet qualification requirements will not automatically disqualify the entire PEP. The SECURE Act provides a remedy if the PEP can show that it has a corrections program and has taken steps to address the failure.

While PEPs began improving the retirement outlook for employers and employees in 2021, more changes were on the horizon.

THE STORY OF POOLED EMPLOYER PLANS CONTINUES

The SECURE Act was amended by the Securing a Strong Retirement Act of 2022, **commonly referred to as SECURE 2.0**. Several provisions in SECURE 2.0 are favorable to PEPs, effective for plan years beginning after December 31, 2022:

- Section 102 enhances the startup tax credit provided in the SECURE Act for employers with up to 50 employees. The startup credit increases from 50% to 100% of eligible startup costs, with a $5,000 annual cap for the first three years.
- Section 102 also introduces a new credit that applies to employers with up to 50 employees who contribute to new defined contribution plans. A $1,000 credit per employee is currently available, although that amount phases out for employers with 51 to 100 employees.
- **Section 105** clarifies that a PEP may designate a named fiduciary to collect contributions to the plan. Such fiduciary — that does not have to be an employer in the plan — must implement written contribution collection procedures that are reasonable, diligent, and systematic.
- Section 106 extends relief from the "one bad apple" rule mentioned above to 403(b) plans, which are generally sponsored by charities, educational institutions, and nonprofit organizations.
- Section 106 also expands PEP access to 403(b) Plans, allowing access for many nonprofit organizations and educational institutions. Previously, PEPs were only available for 401(k) plans.

While SECURE 2.0 has played a part in improving retirement plan options available to small businesses, some questions remain.

THE STORY OF POOLED EMPLOYER PLANS CONTINUES

The PEPs story wouldn't be complete without mentioning Form PR, as well as clarifying Form 5500 and **annual financial statement audit requirements.**

All pooled plan providers must file a **Form PR (Registration for Pooled Plan Provider)** based on current regulations. This form is filed electronically with the **DOL and IRS through EFAST2**, and the Acknowledgment ID (AckID) issued for the filing can be used to confirm compliance.

As for Form 5500, which must be filed annually, PEPs are required to **file a Form 5500**, not a Form 5500-SF. Individual participating employers do not file separate Forms 5500 for their portion of the PEP; instead, one form is filed that covers all participants in the plan.

Some initial confusion existed over whether the audit threshold for PEPs referred to the entire plan or each participating employer. Under ERISA, employee benefit plans with 100 or more participants are required to conduct an annual audit, and, although structured differently than single-employer plans, PEPs are no exception. The DOL has confirmed that the audit threshold applies to the entire plan and that plans are still subject to the 80-120 rule.

A FINAL WORD ON POOLED EMPLOYER PLANS

Pooled employer plans are not for everyone but can be a game changer for eligible employers and their employees. Our **Employee Benefit Plan Audit team** can help review your ERISA benefits plan, conduct your annual audit, and offer advice on maintaining compliance with existing regulations while keeping watch for additional updates.

Countdown to Compliance: Navigating SECURE 2.0's Plan Amendment Deadlines

Deadlines are quickly approaching for ERISA employee benefit plans. Not only must plan sponsors comply with the provisions set forth in the Securing a Strong Retirement Act of 2022 (SECURE 2.0), but compliance may also trigger mandatory plan amendments that must be adopted according to a timeline set by the IRS. Waiting until deadlines loom to adopt plan amendments can turn a manageable process into a last-minute scramble, especially when procrastination can result in plan disqualification. In this article, we explain the upcoming deadlines and offer advice on taking a proactive approach.

SECURE 2.0 AND ERISA RETIREMENT PLANS

SECURE 2.0 introduced sweeping reforms for employee retirement plans, intended to increase plan coverage while bringing clarity to complicated rules. Some modifications are mandatory, while others are optional; either may require amendments to plan documents.

The Act contains more than 90 changes related to various plan-related issues, including but not limited to the following:

- Increasing catch-up contributions, including new "super" catch ups for participants who are age 60 to 63.
- Rothification of catch-up contributions for participants earning over $145,000 (indexed) starting in 2026.
- Participant election of Roth treatment for employer contributions.
- 401(k) coverage for eligible long-term part-time employees.
- Mandatory automatic enrollment for new 401(k) or 403(b) plans.
- Expanding the Employee Plans Compliance Resolution System (EPCRS).
- Increasing the small employer plan start-up credit.
- Reform of family attribution rules.

It is crucial for employers with qualified retirement plans to understand how SECURE 2.0 affects their plan provisions. For a more comprehensive review, please refer to BDO's previous article, "**Secure 2.0 Act of 2022 Introduces Key Changes for Workplace Retirement Plans**."

A UNIFIED MANDATE WITH DIFFERENT DEADLINES

Under **IRS Notice N-2024-02**, all plans must amend their plan documents by the following deadlines, regardless of whether the plan operates on a fiscal year or calendar year basis, for all changes in the law in the past few years, including the CARES Act, SECURE 1.0 and SECURE 2.0:

- 12/31/2026: Qualified plans, excluding governmental plans or union plans.
- 12/31/2028: Union plans under collective bargaining agreements.
- 12/31/2029: Governmental plans under IRC Section 414(d) and 403(b) plans sponsored by public school.

Amending an ERISA retirement plan requires robust review and decision making, which may include working with outside entities. It's never too early to start, as the process of preparing and finalizing plan amendments can.

BEST PRACTICES FOR PLAN SPONSORS FACING SECURE 2.0 DEADLINES

How can employers and plan sponsors manage their plan amendment process?

Review the plan now.

Conducting a thorough review of current plan documents will help employers and sponsors fully understand the existing provisions and identify potential changes early in the process. If the employer implemented any CARES Act, SECURE 1.0 or SECURE 2.0 changes in the law in operation, those changes must be memorialized in the plan amendment.

Manage third-party collaboration.

When working with third-party vendors or outside service providers, be sure to give them sufficient time to prepare the necessary amendment documents. As work progresses, maintain regular communication with vendors and providers to confirm their work is on track.

Discuss key decisions.

Add SECURE 2.0 reminders to meeting agendas to promote early discussions. Employers and plan sponsors should make key decisions as soon as possible so they are prepared to sign amendment documents when the final documents arrive.

As mentioned earlier, all qualified ERISA retirement plans are subject to the mandatory plan amendment deadlines. Taking a proactive approach to preparing plan amendments can lead to a smoother process and reduce the risk of last-minute complications.

BEST PRACTICES FOR PLAN SPONSORS FACING SECURE 2.0 DEADLINES

Complying with regulations for ERISA retirement plans is never easy, particularly when facing mandatory deadlines. Our **Employee Benefit Plan Audit team** can help review your plan and assist with plan amendments.

Forfeiture Accounts: Why Strong Oversight from Plan Sponsors Matters

Should employers who sponsor 401(k) and 403(b) retirement plans and plan fiduciaries be concerned about plan forfeitures that accumulate, for example, when employees exit before becoming fully vested? More importantly, how should they manage these funds? Allowing forfeiture accounts to build up might be the first mistake, but failing to use the funds appropriately can result in serious consequences.

ERISA retirement plan documents contain provisions covering forfeiture accounts, often drawn directly from IRS proposed regulations issued in February 2023 (which have not been finalized as of publication of this article). In practice, addressing these funds involves more than simply knowing that rules and guidance exist. Plan fiduciaries must also know how to apply these rules to their specific circumstances.

In the following article, we offer key details to help plans manage their forfeiture accounts — starting with an understanding of the rules.

WHERE DO ERISA, THE IRS, AND DOL FIT IN?

Provisions in the Employee Retirement Income Security Act (ERISA) and rules established by the IRS relate to the management of plan forfeitures as follows:

- ERISA requires people or entities with **fiduciary responsibility** over plan assets, including forfeiture accounts, to act only in the interest of participants and beneficiaries.
- IRS rules generally provide three ways for plans to use forfeitures:
  - To pay plan expenses,
  - To reduce future employer contributions, or
  - To increase benefits to participants by allocating the extra funds to participants.

For several years now, plan participants have filed lawsuits claiming that a breach of fiduciary duties under ERISA occurs when forfeiture funds are used to reduce employer contributions. Recently, the **DOL has filed a brief in one lawsuit** indicating support for such use of forfeitures.

Thoughtful oversight and management of plan forfeitures can help plan sponsors and employers avoid the potentially serious consequences of allowing funds to grow unused.

RISKS ASSOCIATED WITH FORFEITURE ACCOUNTS

Plan documents typically specify the use of forfeitures and may require forfeiture balances to be used within a specific time period. Generally, forfeitures must be used by the end of the plan year in which they arise or no later than the end of the plan year following the plan year in which the forfeiture occurred. If those rules, including any plan provisions regarding the timing of using the forfeitures, are not followed and forfeiture balances are allowed to accumulate, this noncompliance can lead to tax qualification issues for the plan.

Additionally, participants and former participants may disagree with the method used by a plan to manage forfeiture accounts. In recent years, over 70 federal lawsuits have been filed related to the usage of forfeitures and whether the usage is considered a breach of fiduciary duty. These lawsuits typically relate to forfeitures used to reduce employer contributions, since that appears to use plan assets to directly benefit the employer. The failure to properly address overgrown forfeiture accounts can open the door to litigation and can lead to complete disqualification of the plan.

While there are risks associated with forfeiture funds, plans also can take steps to mitigate those risks.

PROACTIVE FORFEITURE ACCOUNT MANAGEMENT

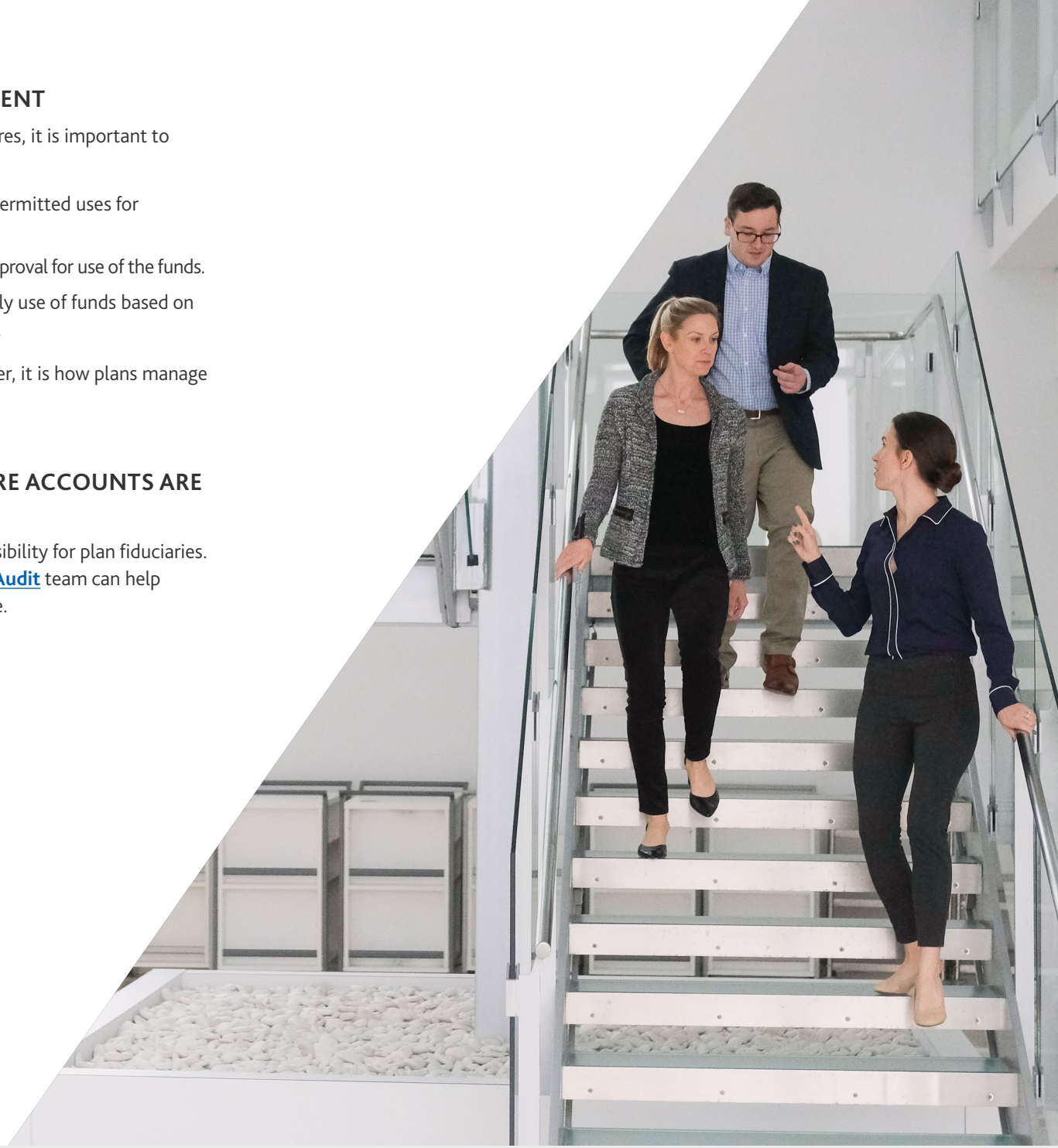
As plan fiduciaries determine how to manage their plan forfeitures, it is important to remember three best practices:

- Review plan provisions related to forfeitures, including the permitted uses for forfeitures and required timing.
- Discuss forfeiture accounts on a regular basis and document approval for use of the funds.
- Monitor account balances at least annually and ensure timely use of funds based on plan provisions to avoid unnecessary accumulation of funds.

Forfeitures are a normal part of ERISA retirement plans. However, it is how plans manage these funds that makes the difference.

DO YOU KNOW HOW YOUR PLAN'S FORFEITURE ACCOUNTS ARE BEING USED?

Thorough, periodic review of plan forfeitures is a critical responsibility for plan fiduciaries. For assistance, please contact us. Our **Employee Benefit Plan Audit** team can help review your ERISA benefits plan and offer comprehensive advice.



Why a SOC 1 Report Matters for Your Organization

When your organization outsources critical business processes—such as payroll, claims processing, or transaction management—to a service provider, you are entrusting them with activities that may directly impact your financial statements. In effect, these outsourced services take the place of your team and the processes you would otherwise maintain in-house. As a result, the same risks to your financial reporting still exist, but the controls to address those risks are now being performed outside your organization. To bridge the gap of understanding and evaluating these controls performed at a service provider, a **SOC 1 report** is often important.

WHAT IS A SOC 1 REPORT?

A SOC (System and Organization Controls) 1 report is a report that includes an independent, **third-party attestation** that evaluates the design and operating effectiveness of a service provider's controls relevant to their clients' financial reporting. It is performed in accordance with AICPA attestation standards. Note that there are other standards, such as ISAE 3402 as well as SOC 2, SOC 3 and a number of others, which are not covered here. Also note that, while a SOC 1 Type 1 report may be helpful in understanding controls at a service provider, a SOC 1 Type 2 report is generally needed to demonstrate controls operating over a period of time at the service provider.

WHY IS A SOC 1 REPORT IMPORTANT?

Assurance Over Outsourced Controls: A SOC 1 report helps to provide assurance that your service provider has effective controls in place to safeguard the integrity of the processes and data that impact your financial statements. This is crucial because, although the work is performed externally, your organization remains responsible for the accuracy of its financial reporting. In other words, you can outsource the service, but you cannot outsource the risk.

Risk Mitigation: The risks to your financial statements do not disappear when you outsource—the actions to address them are simply shared with your service provider. A SOC 1 report helps you understand and evaluate how those risks are being managed and controlled.

Audit Efficiency: External auditors often utilize a SOC 1 report as evidence that appropriate controls are in place at your service provider to address the risks to the financial statements. This can help streamline your annual audit process and reduce the need for additional testing.

Governance and Regulatory and Stakeholder Confidence: Demonstrating that you have obtained and reviewed SOC 1 reports from your key service providers is a key governance step in understanding how the risks to your financial statements are being addressed and further shows regulators, investors, and other stakeholders that you are proactively managing the risk to your financial statements for processes that use third-party services.

WHY IS IT IMPORTANT FOR A COMPANY TO PERFORM AND DOCUMENT A COMPREHENSIVE SOC 1 REPORT REVIEW?

Demonstrates Effective Risk Management and Due Diligence

- Reviewing the SOC 1 report helps identify any control gaps, exceptions, or issues that could impact your organization.
- Documenting your review process provides evidence that you are actively managing third-party risks and fulfilling your oversight responsibilities.

Supports Financial Statement Integrity

- Many outsourced processes directly affect your financial reporting. A careful review helps to ensure that the service provider is operating controls that help to reduce the risk of misstatements in your financial statements.

Satisfies Auditor and Regulatory Expectations, Demonstrates Governance

- External auditors and regulators expect companies to not only obtain but also evaluate SOC 1 reports. Well-documented reviews demonstrate compliance with internal control requirements and practices common in the industry. Whether you work in a regulated industry or not, having governance over the impact third parties have on your financial statements is important.
- SOC 1 report reviews are a critical component of third-party risk management programs. By systematically evaluating the controls and risks associated with service organizations, companies can proactively identify and address potential vulnerabilities. This process not only strengthens oversight of outsourced relationships but also provides assurance to the Board of Directors and Audit Committee that appropriate due diligence and ongoing monitoring are in place to safeguard the organization's operations and reputation.

Identifies User Entity Control Considerations

- SOC 1 reports frequently specify controls that your organization (the user entity) must implement in addition to the service provider's controls. Reviewing and documenting these considerations, and subsequently ensuring you have relevant controls in place, helps to control the risks to financial statements.

Enables Timely Response to Changes and Issues

- A thorough review allows you to promptly address any control deficiencies (sometimes referred to as deviations or exceptions) or changes in the service provider's environment that could impact your operations or compliance.

Provides an Audit Trail

- Documenting your review creates a clear record for internal and external stakeholders, auditors, and regulators, showing how you assessed and responded to risks.

WHAT TO CONSIDER WHEN REVIEWING AND DOCUMENTING YOUR REVIEW OF A SOC 1 REPORT FROM YOUR SERVICE ORGANIZATION

SOC 1 reports are critical tools for understanding the controls in place at your service providers. When you rely on third-party services for key business processes, there are a number of areas to review. The list below includes some of the main areas and considerations you may want to have as you review. The list does not cover all possible considerations.

Scope of the Report

- **Services Covered:** Confirm the report covers the specific services you use. Often a third party provides many different services and as such, it is important the scope covers the relevant services and, if relevant, applications provided.
- **Control Objectives/Criteria:** Review which control objectives are included.
- **Subservice Organizations:** Check if any critical processes are outsourced further (fourth or fifth parties, otherwise known as subservice organizations) and how they are addressed (carve-out: The service auditor's report excludes controls at the subservice organization; the user entity is responsible for evaluating those controls separately vs. Inclusive method: The service auditor's report includes and tests relevant controls at the subservice organization, providing a more comprehensive view within the main report).

Report Period and Timeliness

- **Period Covered:** Ensure the report covers the period relevant to your audit or review. Does the report cover a sufficient amount of time from your fiscal year and/or for your audit period? Should a bridge letter from the service provider be requested, obtained, and reviewed?
- **Type 1 vs. Type 2:** Type 1 reports assess controls at a point in time; Type 2 reports assess operating effectiveness over a period (typically more valuable for audits).

Auditor's Opinion

- **Unqualified Opinion:** Indicates controls were suitably designed and (for Type 2) operating effectively.
- **Qualified/Adverse/Disclaimer:** Understand the nature and impact of any qualifications or disclaimers. If you have mapped your risks to a control objective that may be qualified in the opinion, your ability to rely on the report may be impeded and likely further follow up with the service provider will be helpful.

Reputation and Qualification of the Service Auditor

- Confirm that the service auditor issuing the SOC 1 report is a licensed CPA firm with a strong reputation and recognized expertise in the market. Engaging a reputable and experienced auditor enhances the reliability of the report and provides greater assurance that the procedures performed meet professional standards, allowing you to place appropriate reliance on their findings.

Reading and Understanding Control Descriptions

- **Why It's Important:** Fully reading the control descriptions in the SOC report helps you understand exactly how each control operates and how it aligns with your expectations and requirements.
- **Align with Expectations:** Assess whether the described controls address your organization's needs and risk areas. Don't assume that they do—it is important to confirm that the control activities are sufficient for your reliance.
- **Understand the Control Framework:** Gain insight into the service provider's overall control environment, including entity-level controls that set the tone for effective risk management.
- **Document Your Review:** Keep a record of your review process, noting any questions.

Risk & Control Mapping

- **Why it Matters:** Not all SOC reports are created equal. It's essential to confirm that the report addresses the specific risks associated with the services you use—and that the controls implemented by the service provider and tested by the service auditor align with those risks.
- **Map Your Risks:** Identify the key risks related to the outsourced services you receive
- **Match Controls:** Review the SOC report to confirm the controls tested by the auditor directly address those risks
- **Gaps:** If you find that certain risks are not covered, consider additional due diligence or request clarification from the service provider or, when permissible, the service auditor.

Information Produced by the Entity (Key Reports) Service Auditor's Procedures

- Review how the independent service auditor evaluated the completeness and accuracy of reports (sometimes referred to as Information produced by the entity or IPE) used in control activities. This may include:
- Testing the source of the data.
- Verifying parameters used to generate reports.
- Re-performing calculations or data extraction.
- Reviewing access controls over report generation.

- **Documentation in the SOC Report:** The SOC 1 report should describe the procedures performed by the auditor to assess each relevant IPE's completeness and accuracy. Look for explicit references in the control descriptions and test procedures/results.
- **Exceptions or Issues:** Note any exceptions identified by the auditor related to IPE. These could impact the reliability of controls and, ultimately, your reliance on the service organization.

Complementary User Entity Controls (CUECs)

- **Your Responsibilities:** SOC reports often list controls that are the responsibility of the user organization (that is, your organization). Review these carefully and ensure you have implemented them and tied them back to your key controls. Your own system of internal controls should appropriately reflect the operation of those controls (CUECs) that are critical to the achievement of the control objectives in the SOC 1 report, so it will be beneficial to map the CUECs in the SOC 1 report to the controls at your organization that satisfy the considerations noted.

Complementary Subservice Organization Controls (CSOCs)

- In addition to CUECs, SOC reports may also identify CSOCs—controls that the subservice organization (e.g., a critical vendor or outsourced provider) is expected to have in place to achieve certain control objectives. It is important to understand which controls are designated as CSOCs and to assess whether the subservice organization has implemented them effectively. Where possible, obtain assurance (such as through a SOC report from the subservice organization) that these controls are operating as intended, as your organization may rely on them to meet its own control objectives.

Test Procedures, Results, and Exceptions

- **Control Testing:** Review the auditor's testing procedures and results for each relevant control. The relevant controls are those you noted in the mapping of your risks to the control objectives in the report.
- **Procedures:** Evaluate to determine if the testing steps are sufficiently robust to test the controls in lieu of your organization performing its own procedures.
- **Exceptions/Deviations:** Note any exceptions or control failures and assess their impact on your organization.
- **Management Response:** Check if the service organization has addressed any exceptions.

Ongoing Monitoring

- **Annual Review:** SOC reports should be reviewed as frequently as deemed necessary by management. Often, they are reviewed annually or when significant changes occur.
- **Communication:** Maintain open communication with your service provider regarding control changes or incidents.

Ensuring a thorough review and documentation of SOC 1 reports is essential for effective risk management, audit readiness, and stakeholder confidence. If you need guidance interpreting SOC reports or strengthening your third-party risk oversight, BDO's Information System Assurance team is here to help.

A SOC 1 report provides critical assurance that outsourced service providers - such as those managing payroll or claims processing - have effective controls in place, which directly supports the integrity of benefit plan financial reporting. By reviewing and documenting SOC 1 reports, plan sponsors can demonstrate strong governance and due diligence, helping to mitigate risk and maintain compliance with fiduciary responsibilities under benefit plan regulations. If you'd like to learn more, or have questions about your current SOC 1 report, please reach out our **Employee Benefit Team**.

CONTACT US

ERIN BREIT
Assurance Principal
Employee Benefit Plans
ebreit@bdo.com

KAROLYN LADAS
Assurance Principal
Employee Benefit Plans
kladas@bdo.com

NORMA SHARARA
National Tax Managing Director
Compensation and Benefits
nsharara@bdo.com

NICOLE PARNELL
Global Employer Serices Principal
Retirement Plan Services Leader
nparnell@bdo.com

BOB HAMILTON
Senior Director
Employee Benefit Plans
bhamilton@bdo.com

MARY ESPINOSA
Assurance Principal
Employee Benefit Plans
mespinosa@bdo.com

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.