

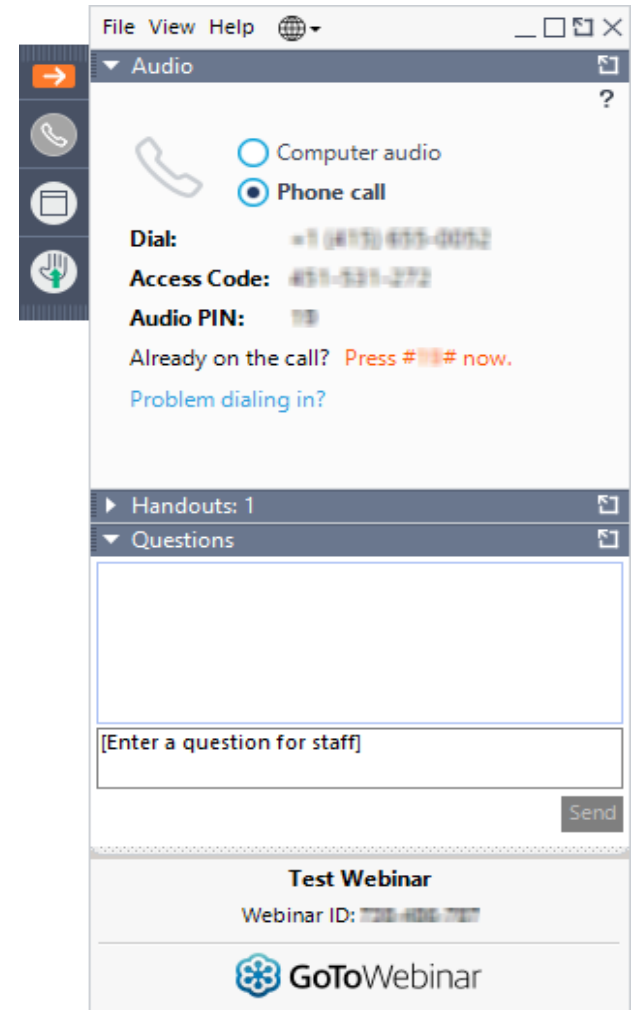
FIDUCIARY TRAINING PART IV: STAYING AHEAD OF RETIREMENT PLAN AUDITS

November 2023



Information About Today's Session

- Select “Phone call” to dial in.
- All attendee lines are automatically muted.
- Questions can be asked by typing them into the questions pane on the control panel, and there will be time at the end of the session to answer questions.
- Submitted questions will not be visible to other audience members.
- Today's session is being recorded.





DAWN MCPHERSON



Director, Retirement Plan Consulting
CAPTRUST



dawn.mcpherson@captrust.com



SUSAN SHOEMAKER



Principal, Financial Advisor
CAPTRUST



Susan.shoemaker@captrust.com



JODI GREEN



ERISA Attorney and Partner
Tatum Hillman & Powell, LLC



jgreen@thplawfirm.com



SCOTT MILLER



CPA and Retirement Plan Auditor
Scott Miller CPA & Associates, Inc



scott@scottmillercpa.com

FIDUCIARY TRAINING PART IV: STAYING AHEAD OF RETIREMENT PLAN AUDITS

November 2023



Department of Labor (DOL) Audits: Triggers & Tips

Potential audit triggers:

- High number of terminated participants with vested balances
- Late contributions
- Outdated or incomplete participant data
- Excessive fees paid to service providers

Tips:

- Know Employee Benefits Security Administration's (EBSA) primary and current areas of focus
- Be aware of current litigation
- Maintain participant census data
- Take advantage of the DOL's Voluntary Fiduciary Compliance Program (VFCP)
- Review Form 5500
- Add further explanation and notes in the auditor's report

Cybersecurity

A plan sponsor should:

- Test cybersecurity of their own systems
- Assess insurance that covers cybersecurity
- Evaluate cybersecurity by asking questions to third-party providers

A third-party provider should:

- Ensure legal standards are met
- Regularly address evolving vulnerabilities (annually)
- Use a “formal well-documented” cybersecurity program with “procedures, guidelines, and standards” that are “regularly updated” and “actually implemented” (per the DOL)
- Have reliable third-party audits

Changes in CPA Auditing Standards for Retirement Plans

2021 plan year

- Statement on Auditing Standards (SAS) 136 – codified specific procedures to be performed over ‘qualified institutions’, management’s responsibilities, Form 5500 review, and Form 5500 supplemental schedules and changed the auditor’s report. Renamed the “DOL limited-scope audit” to an “ERISA 103(a)(3)(C) audit”

2022 plan year

- SAS 142 – codified specific procedures auditors are required to perform in assessing audit evidence obtained and its appropriateness, sufficiency, and persuasiveness

2023 plan year

- SAS 145 – codified specific procedures auditors are required to perform related to information technology (IT) controls and risk assessment

Common Retirement Plan Failures

Top Ten Failures

1. Failure to amend the plan for tax law changes by the end of the period required by the law
2. Failure to follow the plan's definition of compensation for determining contributions
3. Failure to include eligible employees in the plan or failure to exclude ineligible employees from the plan
4. Failure of plan loans to comply with Internal Revenue Code (IRC) section 72(p)
5. Impermissible in-service withdrawals
6. Failure to satisfy IRC 401(a)(9) minimum distribution rules
7. Failed employer eligibility
8. Failed Actual Deferral Percentage (ADP)/Actual Contribution Percentage (ACP) nondiscrimination tests under IRC 401(k) and 401(m) not corrected in a timely manner
9. Failure to properly provide the minimum top-heavy benefit or contribution under IRC 416 to non-key employees
10. Failure to satisfy the limits of IRC 415

Source: IRS Top Ten Failures Found in Voluntary Correction Program

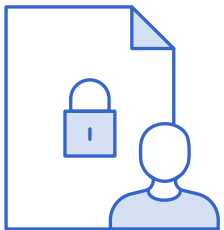
What Is a SOC Report?

A SOC (System and Organizational Controls) report is an independent audit report performed by a certified public accountant (CPA).



SOC 1

- Focuses on an organization's internal control over financial reporting
 - Type I – auditor's evaluation of the design and appropriateness of internal control systems to meet the organization's objectives
 - Type II – includes components of type I and the auditor's evaluation on operating **effectiveness** of the controls



SOC 2

- Focuses on how an organization secures and protects client data

Takeaways

1 Review plan document annually to ensure you're following plan terms

2 Stay current on the regulatory and litigation landscape

3 Document meetings and decisions

4 Hire the right experts to assist

Resources

Employee Benefits Security Administration

- [Programs and Initiatives | U.S. Department of Labor \(dol.gov\)](#)
- Review *National Enforcement Projects*
- [Fact Sheets | U.S. Department of Labor \(dol.gov\)](#)

Department of Labor

- [Cybersecurity | U.S. Department of Labor \(dol.gov\)](#)

Internal Revenue System

- [401\(k\) Plan Fix-It Guide | Internal Revenue Service \(irs.gov\)](#)



QUESTIONS

THANK YOU!

Disclosure

This document is intended to be informational only and does not constitute legal, accounting, or tax advice. Please consult the appropriate legal, accounting, or tax advisor if you require such advice. This content is not a solicitation or an offer to buy any security or instrument or to participate in any trading strategy. Any performance data quoted represents past performance. Investment return and principal value of an investment will fluctuate so that an investor's shares, when redeemed, may be worth more or less than their original cost. Past performance is no guarantee of future results.

All publication rights reserved. None of the material in this publication may be reproduced in any form without the express written permission of CAPTRUST: 919.870.6822.