ALLIANT WEALTH ADVISORS

Qualified Plans Division

TRAILBLAZER

Blazing a Path Toward Retirement

How to Prepare for a 401(k) Audit

–

Diversity, Equity and Inclusion and Their Impact on Retirement Plans

–

Cybersecurity Best Practices for Plan Sponsors

Q1 2022

News and Information for Employers

Fiduciary Plan Governance Edition

HOW TO PREPARE for a 401(k) Audit

If the DOL comes knocking, is your plan prepared for an audit? Be aware of red flags, how to respond and what documents to have ready.

#DOL #Audit #401k

If the term "audit" makes you uncomfortable, anxious or even scared, you are not alone. Last year, the Department of Labor (DOL) closed 1,122 civil investigations with 754 (67%), resulting in fees, repayments or corrective actions.[1] The agency collected over $3.12 billion in direct payments to plans, participants and beneficiaries. This represents a whopping 300% increase in just five years.[2]

From this perspective, you might think there is no chance that you're walking out of an audit unscathed. However, the outlook is a little less bleak when you realize that in the US, there are nearly 722,000 retirement plans and only 1,122 escalated to investigation.

So instead of viewing the DOL as the boogey monster or fearing a 401(k) audit, let's take a look at the utility behind audits, identify red flags and establish best practices to help demystify the process.

WHAT IS A 401(K) AUDIT?

Retirement plan audits are normal; in fact, they happen all the time. Generally speaking, a plan audit is the review of a company's retirement plan with the primary objective of ensuring that it meets guidelines and regulations set by the DOL and IRS. For large companies with over 100 participants, audits are an annual occurrence, but small plans can also be under scrutiny if a red flag is raised.

WHAT ARE AUDIT RED FLAGS?

The following red flags can prompt the DOL to take a closer look at your retirement plan.

Employee Complaints

Individual complaints from employees are a frequent source of DOL investigations. From a total of 171,863 inquiries from workers, 357 resulted in the opening of new investigations and more than half of all monetary recoveries relate to benefits of terminated vested participants of defined benefit plans.[3] The simple lesson here is that plan sponsors must establish clear protocols for how participants can communicate questions or complaints about their benefits to the plan sponsor before filing complaints with the DOL. Quick and effective responses are critical.

DOL Enforcement Priorities

Examinations may also relate to enforcement priorities launched by the DOL. As of this publication, the agency "continues to focus its enforcement resources on areas that have the greatest impact on the protection of plan assets and participants' benefits."[4] Recent priorities include plan sponsors' attention to the cybersecurity policies of their service providers and their tracking of terminated participants.

1 Department of Labor. "Fact Sheet. EBSA Restores Over $3.1 Billion to Employee Benefit Plans, Participants and Beneficiaries." 2020.

2 Ibid.

3 Ibid.

4 Employee Benefits Security Administration. "Enforcement." DOL.gov. Accessed 2021.

Delinquent Contributions

Delinquent contributions are pursued as part of an ongoing national priority. These are easy pickings for the DOL and a clear violation of the most basic fiduciary standards. This should be done within the given year's contribution-eligible time period and at a consistent time each pay to avoid attention from the IRS/DOL.

Plan sponsors are encouraged to review their Form 5500 and other records to spot trouble points, such as:

- Missed contributions
- Assets not held in trust
- Paying unreasonable compensation to service providers (conduct regular fee benchmarking to avoid this)
- Paying expenses from the plan that are actually expenses of the employer (known as "settlor expenses". These costs include consulting services regarding plan design or plan termination.)

Other areas of interest include lost or missing participants, and, of course, the DOL often accepts referrals from other agencies such as the IRS.

A KNOCK AT THE DOOR

If you happen to receive a notice from the DOL about an audit or an investigation, your response should be the same:

- Take a deep breath.
- Put your team together and choose a qualified primary contact person.
- Strongly consider engaging ERISA counsel. Expert help may avoid missteps and provide an intermediary for difficult conversations.
- Consider requesting an extension of time to respond. Many initial deadlines can be short for complex exams. Extensions, if reasonable, are routinely granted.
- Review all documents prior to production. Be ready to report any issues found.
- Deliver documents in neat and organized fashion.
- Prepare employees for interviews. Treat it like a deposition. Caution them to take their time, thoughtfully consider their responses and ask for clarification of any questions they do not understand.
- Always be truthful and respectful.

WHAT DOCUMENTS ARE TYPICALLY REQUESTED?

The sheer volume of documents requested may at first seem overwhelming, but the requests will be for documents you should have readily available in your files. They include:

- Plan document, Investment Policy Statement, plan records of fees/expenses
- Form 5500, Summary Plan Description (SPD), Summary Material Modification (SMM), participant fee disclosures and benefit statements
- Service provider contracts and fee disclosures
- Participant claims and benefits data
- Bonding and fiduciary liability insurance
- Fiduciary committee charters, committee meeting minutes and other records
- Organizational documents about your company and organizational charts
- More recently, cybersecurity practices

STAY PREPARED

Whether you are subject to a routine audit or a red flag prompts an investigation, it is important to remember that fiduciary vigilance is key. The best preparation is to follow sound operational procedures every day and don't fall behind.

DIVERSITY, EQUITY AND INCLUSION and Their Impact on Retirement Plans

Your workforce is diverse and unique — how does your retirement plan reflect DEI efforts?

#DEI #401k #FinancialWellness

Today's workforce spans a variety of abilities, skills, experiences and cultural backgrounds that bring exceptional value. It is beneficial to understand and recognize these differences to achieve exceptional results. This remains true when offering, communicating and promoting your company's retirement plan.

RAISING AWARENESS

Thankfully, your retirement plan is no stranger to reporting. From participation rates, deferral percentages, asset allocation mixes, benchmarking analysis, investment reviews and other slice and dice metrics, retirement plan information is often shared based on your plan's specific numbers and peer group comparison.

However, those calculations seldom include the lens of Diversity, Equity and Inclusion (DEI). Now all that is changing.

EXPANDING THE SCOPE

Nearly two-thirds of plan sponsors have noticed an increased demand for retirement plans to align with DEI efforts.[1] So, now is a good time for employers and retirement plan committee members to revisit and re-evaluate how their 401(k) plans align with the workplace climate.

Four primary areas to review your workplace retirement plan DEI may include:

Participant cohorts: Participants save and accumulate assets differently. Take a look at your company's demographics to spot under savers (participation, deferral, asset allocation, etc.). Then implement a targeted strategy to help all groups take advantage of the opportunities offered by your plan.

Committee composition: To foster a deeper understanding of your employees' savings experience, reassess and consider expanding the retirement plan committee to include a representative structure that mirrors your workforce, potentially bringing greater insights that enhance retirement savings.

Investment offering: Consult with us for a review of your investment menu and discuss how a DEI strategy could be reflected throughout your retirement plan's investment offerings.

Holistic mindset: For the majority of Americans, the workplace retirement plan is their primary savings and accumulation vehicle for retirement. Employers and committee members should address the current financial state of plan participants to ensure the diverse needs of their workplace are being addressed. Boosting the financial wellbeing of plan participants can drive the improvement of plan outcomes and allow all demographic groups to better engage with the benefits offered to them.

FINANCIAL WELLNESS

DEI is an essential part of a financial wellness program. A financial wellness program's purpose is to help employees improve their overall financial situation. The best way to do this is by gaining an understanding of the differences that may exist between diversity groups (e.g. age, race, ethnicity, gender, physical abilities, sexual orientation, etc.), followed by viewing plan data to identify cohorts that could benefit from receiving additional resources. Sponsors can also use the data presented to look at demographic groups and see if they have different engagement levels in the plan.

One idea to address participation gaps is auto-enrollment. It is agnostic across all employees; it has been found that when auto-enrollment is implemented with Black, Latinx and White Americans, the participation rate remains 80% across the board.[2] Interestingly, when given the same auto-enrollment default, everyone saves the same when they have access. This is one example of how employers can address a coverage issue and, if applicable, address a racial disparity within 401(k) plan participation.

FINANCIAL EDUCATION

Diversity can extend not only to different cultural groups but varying generations as well. As such, employers should offer financial education resources that appeal to the different learning preferences (and languages) of each cohort along with best way to communicate with them about retirement, all while working to improve experiences through effective DEI.

As the lifestyles and stages of employees evolve, so do their financial needs and priorities. For a retirement program to be successful, employers should take these changes into consideration.

One size doesn't fit all. Plan sponsors should seek to employ a mix of communications — utilizing brochures, emails, videos, infographics, blog articles and online calculators — to get the message out to different demographics within the plan.

NEXT STEPS

To get started with your DEI strategy, consider these best practices:

Know your employees: Seek to understand their differing demographics and assess participant behaviors from multiple perspectives.

Talk with your service providers: Set up a meeting to learn what resources are readily available (e.g. financial wellness programs, plan data, different language options, etc.).

Communicate with purpose: Your communications should highlight your retirement plan as a valuable benefit. Help your diverse workforce understand why it is important to save and how your company is helping to promote retirement preparedness.

Using DEI to guide plan decisions can help ensure your company's retirement plan is working to positively impact the different cohorts of your employees. DEI used wisely can increase the retirement engagement and security of all.

1 Willis Towers Watson. "Moving the needle on defined contribution plans." Willis Towers Watson. 27 May 2021.
2 American Retirement Association. "Building on Bipartisan Retirement Legislation: How Can Congress Help?" 28 July 2021.

CYBERSECURITY Best Practices For Plan Sponsors

Your plan data and private information are valuable. Here are 11 key questions you should be asking your 401(k) service providers about the cybersecurity of your retirement plan data.

#Cybersecurity
#RetirementPlan
#Data

Cybersecurity is a critical but often overlooked aspect of a plan sponsor's fiduciary responsibility. In simple terms, cybersecurity means protecting sensitive plan and participant data — and by extension, your participants' financial well-being and retirement security — against attacks from hackers and cyber criminals.

THE DEPARTMENT OF LABOR HAS OUTLINED 12 CYBERSECURITY BEST PRACTICES:

1. Have a formal, well documented cybersecurity program.

2. Conduct prudent annual risk assessments.

3. Have a reliable annual third party audit of security controls.

4. Clearly define and assign information security roles and responsibilities.

5. Have strong access control procedures.

6. Ensure that any assets or data stored in a cloud or managed by a third party service provider are subject to appropriate security reviews and independent security assessments.

7. Conduct periodic cybersecurity awareness training.

8. Implement and manage a secure system development life cycle (SDLC) program.

9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.

10. Encrypt sensitive data, stored and in transit.

11. Implement strong technical controls in accordance with best security practices.

12. Appropriately respond to any past cybersecurity incidents.

TO HELP MAINTAIN YOUR FIDUCIARY RESPONSIBILITY, HERE ARE 11 KEY QUESTIONS YOU SHOULD BE ASKING YOUR 401(K) SERVICE PROVIDERS ABOUT CYBERSECURITY:

1. What are your procedures for dealing with cybersecurity threats and protecting participants' personal information?

2. Do you conduct periodic risk assessments to identify vulnerabilities to cybersecurity threats and the impact of potential business disruptions?

3. Do you conduct an annual, independent assessment of your cybersecurity systems and policies?

4. Can you describe how plan and participant data is encrypted (census upload, enrollment, payroll uploads, transfers and other data exchange policies)?

5. What are your procedures for notifying us of a system breach?

6. Does your company carry cybersecurity insurance? If yes, can you provide an overview of the coverage (including all limitations)?

7. Has your company experienced any security breaches? If yes, explain.

8. How do you store, retain, and destroy sensitive data?

9. Does your company outsource any services to a subcontractor? If yes, what controls are in place to protect our company's sensitive data?

10. Do you have a privacy and security policy, and does the policy apply to personally identifiable information of retirement plan clients?

11. Does your business continuity and disaster recovery plan include the recovery of an employer's data after a breach?

Cybersecurity concerns us all. Whether you are a small business owner or the CEO of a Fortune 100 company, ask your 401(k) service providers these questions and document their responses, because knowing what could cause a data breach is the first step in preventing one.

BLAZING A PATH Toward Retirement

We are dedicated to going the extra mile to make retirement planning simple for you and your employees. When you partner with us, you have experience and innovation in your corner. We strive to help you reduce your fiduciary liability exposure, improve your employees' ability to build toward retirement and provide a hassle-free solution for plan compliance and administration.

ALLIANT WEALTH ADVISORS

Qualified Plans Division

Toll Free: (866) 364-6262 | Fax: (703) 878-9051

MANASSAS OFFICE

9161 Liberia Avenue
Suite 100
Manassas, VA 20110
Office: (703) 878-9050

RESTON OFFICE

11921 Freedom Drive
Two Fountain Square Suite 550
Reston, VA 20190
Office: (703) 904-4388