



SPRING CLEANING

Spring will arrive soon, promising new growth and a fresh beginning. It could also be the perfect time to do some spring cleaning for your plan. Let's look at some areas that you might consider reviewing to ensure your retirement plan is operating efficiently.

Winter 2026

Document your **processes and procedures** to make certain that plan tasks can be handled in case of any absences during an enrollment or pay period. Having a backup in place can prevent errors and delays that could lead to penalties.

Make sure to have a process in place to notify all **new enrollments** of their eligibility, regardless of whether the plan has automatic enrollment. Depending on the timing for plan entry, including the plan enrollment paperwork with the new hire paperwork could make entry easier for you. Please reach out with any questions regarding when an employee enters the plan.

Deposits of employee deferrals and loan repayments must be submitted to the plan as soon as possible to avoid penalties and corrections. For plans with less than 100 participants, a safe harbor rule allows deposits to be made within seven business days. For larger plans, the expectation is that the money will be deposited more quickly. Depositing these funds on the pay date will avoid the possibility of being late.

Monitoring **deferral contribution limits** during the calendar year will avoid refunds after year end. Make sure that your payroll is set up to stop deferrals once the limit is reached, including any catch-up contributions for those who have reached age 50.

To keep the plan in compliance, **employer contributions** must be deposited timely. Due dates are impacted by the type of contributions, required status and tax deductibility. If you have questions on when to deposit your employer contribution or even whether to make an employer contribution, please contact us.

Most plans must be covered by a **fidelity bond**. The minimum coverage is 10% of plan assets (rounded up to the next \$1,000) and the maximum coverage is \$500,000. Additional requirements apply to plans with employer securities or non-publicly traded assets. If your fidelity bond is insufficient, now is the time to raise

the coverage. Inflation clauses that increase the bond amount as the plan assets increase can ensure that your bond coverage is always adequate. Contact us or your insurance provider if you don't have a fidelity bond.

Another area to review is **communication with participants**. Helping your employees understand and trust the plan can increase their contributions. Be sure that your procedures include distributing any plan-related communications—including required participant notices.

Distributions also involve communication, including some of the aforementioned notices. Discussing distribution options with terminated participants, possibly as part of an exit interview, can help to reduce risk of lost participants. We'll provide instruction on distributions for force-out distributions for small balances, testing corrections and required minimum distributions.

Your **plan document** is the legal source on how the plan should be administered; operating within its parameters is critical. It's always worth taking time to review the plan document to ensure that you fully understand and are following its provisions. We'll cover more details about the plan document later in this newsletter.

We're here to support you in keeping your plan in compliance. Please feel free to reach out with any questions.

Cybersecurity & ERISA Compliance: Protecting Your Plan

Cybersecurity has become a necessary consideration in many aspects of life, and your retirement plan is no exception. For plan sponsors, understanding your responsibilities—as well as those of the third party administrators (TPAs) and recordkeepers that you work with—is a fundamental part of ERISA (Employee Retirement Income Security Act) compliance and the fulfillment of your fiduciary responsibilities. Retirement plans hold significant financial assets and large volumes of highly sensitive participant data, making them an attractive target for cybercriminals. As a result, the protection of this data and access to it has become inseparable from the obligation to act prudently and in the best interests of participants.

Why Cybersecurity Matters

Under ERISA, fiduciaries are required to act with care, prudence and diligence when administering a plan and safeguarding its assets. In today's environment, plan assets include not only the money held in trust, but also the systems, data and processes that control access to those assets. Cyber incidents such as account takeovers, fraudulent distributions and data breaches can directly harm participants and may be viewed as a failure of fiduciary prudence. The DOL (Department of Labor) has reinforced that managing cybersecurity risk is now an expected part of plan governance—not an optional enhancement. A failure to consider known and growing cyber risk can expose plan sponsors to regulatory scrutiny, participant claims and reputational damage.

Your Role in Cybersecurity

For plan sponsors, cybersecurity is closely tied to the duty to prudently select and monitor service providers. Sponsors are expected to understand how TPAs and recordkeepers protect participant data, prevent fraud and respond to incidents; evaluating these practices has become just as important as reviewing fees, services and operational capabilities. Let's look at what role each has in protecting your plan:

- TPAs play a critical role in the administration of your plan and routinely handle sensitive participant information and transactional data. As such, we are expected to maintain strong internal controls, secure workflows and documented policies designed to protect plan operations from cyber threats.
- Recordkeepers are often the primary point of interaction for participants and therefore sit in the front line of cybersecurity risk. For them, secure participant access, identity verification, transaction monitoring and distribution controls are essential to protecting retirement savings.



Bottom Line

The Department of Labor's cybersecurity guidance underscores the expectation that plans and their service providers will maintain formal security programs, protect data through appropriate controls, prepare for incidents and clearly communicate with participants. To see the DOL's Cybersecurity Program Best Practices, please visit the URL provided at the end of this article. Following these principles help demonstrate procedural prudence and supports compliance with ERISA's fiduciary standards.

Ultimately, effective cybersecurity protects participants, strengthens trust in the plan, and reduces fiduciary and operational risk. In the current regulatory and litigation environment, sound cybersecurity practices are a clear reflection of prudent plan management. As your TPA, we take digital security seriously, and we are fully committed to protecting your plan and participants and giving you one less thing worry about.

Source: Department of Labor | Cybersecurity Program Best Practices: <https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices>

The Plan Document: Why Understanding it Matters

An employer-sponsored retirement plan is an extremely valuable benefit a company can offer its employees. At the heart of this benefit is the plan document—the official rulebook that explains exactly how the plan works. For plan sponsors, understanding this document isn't just helpful; it's essential. Here's why:

It keeps the plan compliant.

The plan document spells out the rules that make the plan comply with government laws and regulations. These rules cover everything from eligibility requirements to contribution limits

and distribution options. If the company doesn't follow these rules, it could face serious consequences, such as fines, audits or even the loss of the plan's tax advantages. By knowing what the document says, plan sponsors can make sure the plan stays in compliance and avoid costly mistakes.

It helps you run the plan.

The plan document provides clear instructions on how the plan should operate day-to-day. It explains who can enter the plan, when they can enroll, how contributions are calculated, and when employees can withdraw their account balance. If these rules aren't followed, errors can occur—such as enrolling someone too early or miscalculating contributions. Such mistakes can be expensive and time-consuming to fix. Understanding the document helps sponsors keep their plan running smoothly.

It protects employees and the plan sponsor.

Plan sponsors have a fiduciary responsibility, which means they are obligated to act in the best interest of employees. Knowing the plan's provisions ensures that decisions about investments, distributions, and other plan features are made fairly. This not only protects employees' retirement savings but also helps the company avoid potential legal challenges.

It makes changes easier.

Laws and company policies evolve over time, and retirement plans often need to be updated to reflect changes. If plan sponsors understand the current plan provisions, they are better equipped to make updates more efficiently and avoid creating conflicts or gaps in the rules. This proactive approach keeps the plan flexible while remaining compliant.

It improves communication.

Employees will have questions about their retirement benefits. When can they start contributing? When are they eligible for a distribution? Plan sponsors who understand the plan document can provide clear, accurate answers. This builds trust and helps increase employee confidence in their retirement planning.

As you can see, the plan document isn't just paperwork—it's the foundation of the retirement plan. For plan sponsors, understanding the plan document means staying compliant, avoiding costly errors, protecting employees, and ensuring smooth operations. As your TPA, we're here to help you build this foundation and maintain a successful benefit for you and your staff.

Understanding RMDs: What Plan Sponsors Need to Know

As a plan sponsor, it's critical to understand the rules surrounding Required Minimum Distributions (RMDs) because they directly impact compliance, participant education and operational processes. RMDs are mandatory withdrawals from qualified retirement accounts, and failure to handle them correctly can lead to penalties for participants and fiduciary risks for your plan.

In general, **participants who turned age 73 in 2025** are mandated to take their first RMD from qualified retirement plans. This requirement stems from the SECURE Act 2.0, which raised the RMD age from 72 to 73 starting in 2023. For employees born in 1960 or later, the RMD age will increase to 75 in future years. Awareness of the shifts in these age thresholds is necessary for identifying which participants are affected in any given year. Please note that distributions from an IRA will not satisfy the requirement for an RMD from a qualified plan.

For qualified retirement plans, if the plan document allows it, most active employees have the option to delay RMDs until they retire. However, a 5% owner of the business must begin distributions at the appropriate age regardless of employment status. Plan sponsors should ensure these distinctions are clear. The 5% ownership threshold includes ownership attributed from other family members.

Your role is to make sure the plan complies with IRS rules. In terms of RMDs, your responsibilities will include:

- **Identifying affected participants:** Work with us to flag employees who have reached RMD age, as well as any 5% owners who haven't retired.
- **Communicating deadlines and amounts:** Provide clear instructions to participants about when and how much they need to withdraw.
- **Monitoring distributions:** Confirm that you have methods in place for tracking and processing RMDs to avoid errors.

The timing of RMDs is critical. Missing these deadlines can trigger penalties:

- A participant's first RMD is due **by April 1 of the year after reaching RMD age.**
- Subsequent RMDs must be completed **by December 31 each year**, creating the possibility of two distributions in the first year.

The RMD amount is calculated based on the prior year-end account balance divided by a life expectancy factor set by the IRS. Plan sponsors don't calculate these amounts directly, but they should understand the process to answer participant questions and verify accuracy.

Failing to take an RMD can result in a **25% excise tax** on the amount that isn't withdrawn. For plan sponsors, improper handling of RMDs can lead to fiduciary concerns and potential IRS scrutiny.

While RMDs are technically a participant responsibility, they also represent a compliance obligation for your plan. By proactively identifying affected employees, confirming administrative processes, and communicating clearly, you reduce risk and support participants in meeting their distribution requirements.