Risk Mitigation in the 401(k) Business: Why "That's What E&O Is For" Isn't Enough

By Ary Rosenbaum, Esq.

When I first started in the 401(k) business, I worked as a lawyer connected with a third-party administrator that was just getting its feet wet in the daily valuation world. This was back when daily valuation was still new enough that many TPAs treated it like an experiment rather than an operational necessity. One poorly trained daily processor made a mistake, nothing malicious, just a lack of experience combined with insufficient oversight. When the error surfaced, one of the owners of the firm, the man who hired me and mentored me, Harvey Berman, summed it up with a line I'll never forget: "That's why we have errors and omissions insurance." Harvey wasn't wrong. Errors and omissions coverage exists precisely because humans make mistakes. But relying on insurance as your primary risk mitigation strategy is like relying on an ambulance to improve your driving skills. Insurance is the last line of defense, not the first. In today's 401(k) landscape, where litigation is constant, regulators are aggressive, and plaintiffs' firms are inventive, risk mitigation has to be deliberate, layered, and baked into the DNA of every plan provider's operation.

The Reality of Risk in the 401(k) Ecosystem

Risk in the 401(k) business doesn't come from one place. It comes from operational failures, regulatory missteps, human error, cybersecurity breaches, contractual misunderstandings, and fiduciary overreach. TPAs, recordkeepers, advisors, payroll companies, and pooled plan providers all sit in a complex web where a mistake by one party can easily become a lawsuit against everyone else in the room. What makes the retirement industry especially vulnerable is that mistakes often don't surface immediately. A failed ADP test, a missed deferral, an incorrect match formula, or a contribution limit error can sit undetected for years. By the time it's discovered, participants may have terminated, records may be incomplete, and correction costs can be substantial. Plaintiffs' lawyers love hindsight, and regulators love patterns. Risk mitigation isn't about perfection; it's about reducing frequency, severity, and exposure.

Training Is Not Optional, It's the First Line of Defense

Most operational failures in the 401(k) business can be traced back to inadequate training. Not bad intentions. Not laziness. Just people being asked to do complex work without being properly prepared. Daily valuation processing, compliance testing, loan administration, hardship reviews, and distributions are not clerical tasks. They require judgment, regulatory knowledge, and an understanding of plan design. Initial onboarding training is not enough. The law changes. IRS and DOL guidance evolves. Case law reshapes expectations. A processor trained five years ago but never retrained is a liability waiting to happen. Continuing education should not be limited to credentialed professionals. Everyone touching plan data should understand not just what they are doing, but why they are doing it and what can go wrong if they get it wrong. Training also reduces risk in a less obvious way: it empowers employees to raise concerns. A well-trained processor is more likely to say, "This doesn't look right," instead of pushing a transaction through because they're afraid of slowing things down.

Process Controls Matter More Than Heroics

Many plan providers rely on "rock stars", employees who know everything, fix everything, and hold everything together. That's comforting until that employee leaves, gets sick, or makes a mistake no one else catches. Risk mitigation requires systems, not saviors. Segregation of duties is boring but essential. The person entering data should not be the same person approving it. Automated checks should exist, but they should never replace human review. Exception reports should be reviewed regularly, not filed away. Procedures should be documented so that consistency doesn't depend on memory. When regulators investigate failures, they don't ask whether someone

meant well. They ask what controls existed and whether they were followed. A documented process followed imperfectly is defensible. An undocumented process followed inconsistently is not.

Understanding, and Limiting, Your Fiduciary Role

One of the most dangerous risk areas for plan providers is unintentionally becoming a fiduciary. ERISA fiduciary status isn't determined by titles or disclaimers alone; it's determined by function. If you exercise discretionary authority or control over plan assets or plan administration, you are a fiduciary whether you intended to be or not. TPAs and recordkeepers must be disciplined about staying within their contractual roles. Making recommendations is not the same as making decisions. Providing information is not the same as exercising discretion. Crossing that line, even with good intentions, exposes providers to fiduciary liability they never priced for and never insured properly. Risk mitigation means clear service agreements, consistent practices that align with those agreements, and training staff to know when to stop and push decisions back to the plan sponsor or named fiduciary. Being helpful is good. Being a fiduciary by accident is not.

Insurance Is Essential, but Only as a Backstop

Errors and omissions insurance, fiduciary liability insurance, cyber liability coverage, and crime bonds all play a critical role in risk mitigation. But insurance does not prevent losses; it merely helps pay for them. Insurers also expect insureds to act reasonably. Claims are harder to defend when providers ignore known risks, fail to train staff, or operate without basic controls. Insurance policies also have exclusions, limits, and retention amounts that providers often don't fully appreciate until a claim hits. Cyber policies may exclude social engineering losses. E&O policies may exclude certain regulatory penalties. Fiduciary policies may not cover non-fiduciary services at all. Risk mitigation includes understanding what insurance does and does not cover and aligning operational practices accordingly.

Cybersecurity Is Now an Operational Risk, Not an IT Issue

When I started in the 401(k) business, cybersecurity wasn't a concern because everything was paper and phone calls. Today, it's one of the biggest risk vectors in the industry. Participant account takeovers, phishing attacks, fraudulent distributions, and ransomware incidents can create financial losses and regulatory scrutiny overnight. Risk mitigation requires more than firewalls and passwords. It requires employee training to recognize phishing attempts, procedures for verifying distribution requests, vendor due diligence, and incident response planning. Regulators are increasingly asking not just whether a breach occurred, but whether reasonable steps were taken to prevent it. Cyber risk is also fiduciary risk when participant accounts are involved. Providers that treat cybersecurity as someone else's problem are inviting trouble.

Documentation Is Your Silent Witness

In litigation and audits, documentation matters more than memory. Regulators and courts rely on written records to determine what happened and whether actions were reasonable. Risk mitigation means documenting decisions, communications, corrections, and processes. When an error occurs—and it will—the way it's handled matters. Prompt identification, clear communication with the plan sponsor, proper correction under IRS or DOL programs, and thorough documentation can turn a disaster into a manageable issue. Silence, delay, or improvisation usually makes things worse.

Culture Is the Hidden Risk Factor

The most overlooked element of risk mitigation is organizational culture. A culture that prioritizes speed over accuracy, revenue over compliance, or silence over transparency creates risk no insurance policy can fully absorb. Conversely, a culture that encourages questions, values compliance, and treats mistakes as opportunities to improve reduces risk over time. Harvey's comment about E&O insurance wasn't a dismissal of responsibility; it was a recognition of reality. Mistakes happen. But smart firms don't accept them as inevitable. They invest in training, systems, insurance, and boundaries because they understand that risk mitigation is not about avoiding every error, it's about surviving the ones that occur. In the modern 401(k) business, "that's what insurance is for" is not a strategy. It's a safety net. And anyone who relies on a safety net without building a solid structure above it is eventually going to fall.

The Rosenbaum Law Firm P.C.

The Rosenbaum Law Firm P.C.
734 Franklin Avenue, Suite 302
Garden City, New York 11530
(516) 594-1557

http://www.therosenbaumlawfirm.com