Checklist for 401(k) Plan Fiduciaries

This checklist ensures that fiduciaries fulfill their responsibilities under ERISA (Employee Retirement Income Security Act) and best practices for 401(k) plan management.

1. Plan Governance & Oversight

✅ Fiduciary Responsibilities

- ☐ Ensure each committee member completes fiduciary training each year.
- ☐ Maintain up-to-date committee charters, bylaws, and policies.
- ☐ Keep detailed meeting minutes documenting key decisions.
- ☐ Establish and follow a prudent decision-making process for investments and plan operations.
- ☐ Verify fiduciary insurance coverage (E&O and fidelity bonds) is sufficient.

✅ Plan Document Compliance

- ☐ Review the Plan Document and Summary Plan Description (SPD) every 3 years (or upon regulatory changes).
- ☐ Ensure plan operations match the plan documents and amendments.
- ☐ Distribute required notices and disclosures on time (e.g., Safe Harbor, QDIA, Blackout Notices).

2. Investment Oversight

✅ Investment Selection & Monitoring

- ☐ Conduct an investment policy statement (IPS) review annually and ensure compliance.
- ☐ Evaluate fund lineup performance against benchmarks and peer groups quarterly.
- ☐ Document investment changes, fund removals, and rationale for decisions.
- ☐ Offer a diversified mix of investment options, including low-cost index funds.
- ☐ Regularly assess default investment options (QDIA) suitability.

✅ Fees & Expenses Review

- ☐ Benchmark recordkeeping, investment, and advisory fees against industry averages every 1-3 years.
- ☐ Disclose and review 408(b)(2) and 404(a)(5) fee disclosures for reasonableness.
- ☐ Renegotiate fees with providers if deemed excessive.

3. Service Provider Management

✅ Due Diligence & Monitoring

- ☐ Conduct RFPs for recordkeepers at least every 3-5 years.
- ☐ Assess service levels and performance metrics annually.
- ☐ Review and document any conflicts of interest from service providers.

✅ Cybersecurity & Data Protection

- ☐ Confirm that service providers have cybersecurity policies and an incident response plan.
- ☐ Require annual SOC 2 Type II reports from recordkeepers.
- ☐ Implement multi-factor authentication (MFA) for participant accounts where possible.

4. Participant Outcomes & Communication

✅ Education & Engagement

- ☐ Provide annual participant education sessions on retirement planning.
- ☐ Offer/consider automatic enrollment and auto-escalation to improve participation rates.
- ☐ Ensure participants have access to financial wellness tools and advice.

✅ Monitoring Participation & Loans

- ☐ Track participation rates, contribution levels, and deferral rates quarterly.
- ☐ Review loan and hardship withdrawal activity for excessive usage and take corrective action.

5. Compliance Reporting

✅ Regulatory Filings

- ☐ File Form 5500 before the deadline (End of the 7th month following end of plan year - 9 ½ months with extension).
- ☐ Conduct annual nondiscrimination testing (ADP/ACP, Top-Heavy tests).
- ☐ Ensure timely deposit of employee deferrals (no later than 7 business days for small plans).

✅ Audit & Risk Management

- ☐ Engage an independent auditor if the plan has 100+ participants.
- ☐ Review prohibited transactions and correct any plan errors under EPCRS if necessary.
- ☐ Conduct an operational audit at least annually.

Final Review & Documentation

✅ Annual Fiduciary Checklist Completion

- ☐ Conduct a fiduciary self-assessment annually.
- ☐ Document all reviews, discussions, and actions taken.
- ☐ Retain plan records for at least 6 years, as per ERISA guidelines.