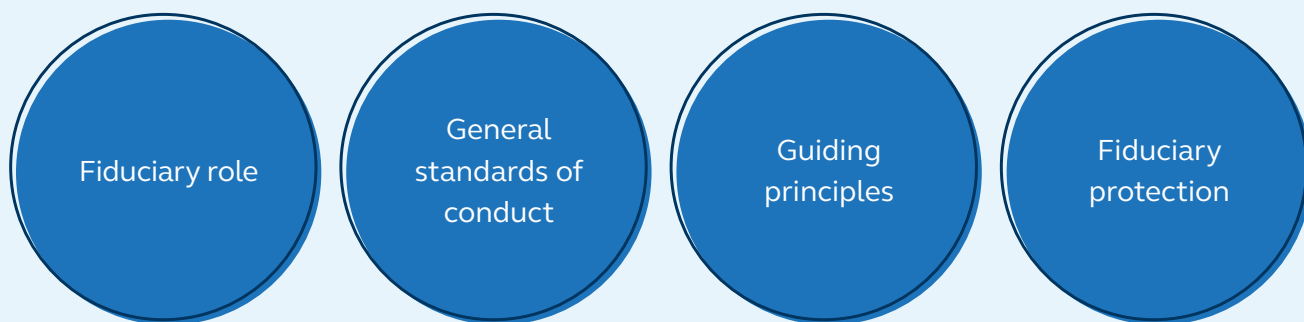

Fiduciary management handbook

Your guide to plan sponsor
and fiduciary responsibilities

Sponsoring a retirement plan comes with significant responsibilities. After all, there's a lot at stake when it comes to helping plan participants save for their best life in retirement. Not to mention the fiduciary duties that come with it.

We've designed this handbook with helpful tips throughout to help you identify and execute your fiduciary responsibilities. By better understanding your role as a fiduciary, you'll gain confidence in meeting your plan objectives and managing your fiduciary risks.

The handbook covers four key areas:



After reviewing this handbook, consult with your financial professionals, third party administrator (TPA), attorneys, accountants, and Principal® representative to answer your specific questions.

Fiduciary role

If you're responsible for managing a retirement plan, you're likely considered an ERISA fiduciary (from the Employee Retirement Income Security Act of 1974). As a named fiduciary, you have the authority to control and manage the operation and administration of the plan, including but not limited to, investments and management of plan assets and expenses (thus, you're held to extremely high standards). Put simply, as an ERISA fiduciary, you're required to act in the best interests of the plan and plan participants.

Here are some general guidelines:

- ERISA requires plans to have one or more named fiduciaries with one individual serving as the plan administrator who is the person with primary responsibility for administering the plan.
- A named fiduciary can be an individual, a group of individuals, a financial professional and/or the employer/organization, and must be listed in the plan document or in whatever manner is described in the plan.
- A committee appointed to manage the plan under the terms of the plan document is also considered a named fiduciary.

Note: ERISA was enacted to protect plan participants' retirement savings by setting guidelines for the operation and investment of retirement plans.

Not all individuals who interact with a retirement plan are considered fiduciaries. For example, accountants, recordkeepers, attorneys, consultants, and others (including employees) who perform purely administrative or ministerial functions aren't ordinarily considered fiduciaries.

The Department of Labor (DOL) provides a five-part test to determine whether a financial representative is a fiduciary advisor. Under the five-part test, a person is considered as providing fiduciary investment advice if he or she provides the investment advice and the advice is:

- 1) Providing the value of investing in securities or other property, or makes recommendations regarding the purchase or sale of securities or other property for a fee.
- 2) Given on a regular basis.
- 3) Pursuant to a mutual agreement or understanding.
- 4) The primary basis for the investment decision.
- 5) Individualized to the needs of the plan.

The DOL may update the definition of a fiduciary sometime this year.

What makes you a fiduciary?

If you're involved in any of the following, it's likely you're considered a fiduciary:

You are named in plan documentation.

You exercise authority or control of plan or asset management.

You provide investment advice for plan assets for compensation such as commissions.

You have discretionary authority or responsibility for plan administration.

You maintain responsibility for plan administration, including:

- Acquiring, holding, disposing, or exchanging investments.
- Managing securities or investments, including recommendations on policies, strategies, portfolio composition, and election of others to provide investment advice or management.

General standards of conduct

As a fiduciary, you have the responsibility to operate a plan solely in the interest of its participants. You must also comply with other specific requirements, including:

- **Exclusive benefit rule:** You must act for the exclusive purpose of providing benefits and paying only reasonable plan fees.
- **Prudent person rule:** You must perform your duties with care, skill, prudence, and diligence that would be exercised by a prudent person familiar with the matter and acting under similar circumstances. When it comes to investment selection, this is sometimes called a prudent expert rule because fiduciaries are measured by the standard of a knowledgeable investor. In other words, a good faith effort without investment knowledge is not enough.

Fiduciaries must engage in a prudent process by gathering and analyzing information before making a decision. If you lack experience, you should seek advice from knowledgeable financial professionals. You should also retain the information received and document the process to protect against a potential breach of duty claim.

- **Diversification rule:** You must diversify the plan investments to minimize the risk of investment loss. When choosing investment options, you should select investments with different objectives and risk/return characteristics. For participant-directed plans, a broad range of investment options should be offered to help participants meet their goals and risk tolerances. (This may not apply to certain plan types holding qualified securities such as an employee stock ownership plan (ESOP).)
- **Duty to follow plan terms:** You must act in accordance to plan documents and ERISA rules. If a plan's documents are in violation of ERISA rules, fiduciaries are required to override the plan document and get their plan in compliance with regulations.

Liability and penalties

Most plan sponsors operate their plan without penalties or lawsuit. But if you do not comply with ERISA, you and the organization sponsoring the plan can face personal liabilities and penalties. That's why it's important to know the rules and key players.

Directly or indirectly, several groups are involved with enforcing ERISA standards, including

- **DOL Employee Benefits Security Administration (EBSA)** — Focuses on fiduciaries meeting their duties.
- **Internal Revenue Service (IRS)** — Oversees rules for operating tax-qualified retirement plans and enforces compliance through plan auditing.
- **Pension Benefit Guaranty Corporation (PBGC)**— Monitors funding adequacy and insures the minimum level of pension benefits for defined benefit retirement plans.

Note: Participants indirectly enforce ERISA when filing claims for benefits or suing fiduciaries for a breach of duties.

Guiding principles

As a fiduciary, not only do you need to take your responsibility seriously, you must also demonstrate you're fulfilling your obligation. It can feel a bit overwhelming, that's why we've broken it down into four guiding principles.



Understand responsibilities



Select and monitor investments



Communicate and educate



Manage prudently



Understand responsibilities

Under ERISA one or more fiduciaries control the administration of a plan on behalf of the participants and beneficiaries. While it's true that plan sponsors typically have some responsibilities considered fiduciary in nature, not all of them fall within this realm.

Here are a few non-fiduciary functions:

- **Designing** and adopting a plan for participants.
- **Evaluating** plan design to make sure it meets goals and objectives.
- **Amending** an existing plan.

The appointment of a named fiduciary and delegation of responsibilities to fiduciaries is a fiduciary act. These appointments are often based on the knowledge, experience, expertise, and role of the individuals within the organization. A common fiduciary delegation is the selection of a financial professional to provide investment advice to the plan and/or participants. When selecting a

service provider/recordkeeper for the plan, it is also important to understand if that service provider will be providing any services as a fiduciary, such as fiduciary investment advice to participants.

When delegating responsibilities to both fiduciary and non-fiduciary service providers, the named fiduciary or plan sponsor should always:

- **Use reasonable and informed judgment** to select or appoint another fiduciary.
- **Evaluate and monitor ongoing performance** of all fiduciaries and other service providers.
- **Maintain a due diligence file** to document information reviewed and decisions made.
- **Schedule ongoing training** about roles, responsibilities and expectations for those involved with the plan (fiduciary and non-fiduciary).

Once appointments have been determined, it's important to inform the named fiduciaries and committee members about the appointments, including descriptions of the positions, expectations and responsibilities, and information about indemnification or liability insurance.

Each individual who accepts an appointment should sign a written confirmation accepting the position

and acknowledging the role with respect to the plan, its participants, and each other.

Keep in mind that delegating responsibilities to others is a fiduciary act. You have the duty to prudently select and monitor these individuals. If you are aware of errors being made by others and do nothing about it, you have co-fiduciary liability with them.



Select and monitor investments

Offering a broad range of diversified and well-selected investment options helps fiduciaries meet their duty to provide investments that are suitable for participants. Once selected, all investments must be monitored. Use these key steps as a guide:

Develop an investment policy statement

An investment policy statement provides a framework to guide fiduciaries in selecting and monitoring plan investment options. Your policy statement should outline a due diligence process, including:

- Criteria for selecting and monitoring investment options
- Guidance for choosing investment managers
- Evaluation of fees

Select investments

Once the plan has defined its investment goals, the investment committee or plan fiduciary can begin the process of choosing a broad range of diverse investment options. While there's no required number of investment options, both the number and type of investments should be appropriate for the plan—including participants' investment abilities.

Regularly monitor investments

Once selected, fiduciaries are responsible for regularly monitoring all plan investments. Investments should be monitored at least annually and when significant events occur. This helps fiduciaries identify and

respond to adverse changes to fees, the investment manager's organization, investment process, or performance results.

If an investment option is no longer deemed prudent for the plan or no longer meets the objectives outlined in the plan's investment policy statement, it may be necessary to replace it with a more suitable alternative. When the appropriate fiduciaries elect to replace an existing investment option, documentation should explain the reason for the removal and rationale for the replacement. Changes should be communicated to participants in advance as required by the DOL ERISA 404(a) regulation.

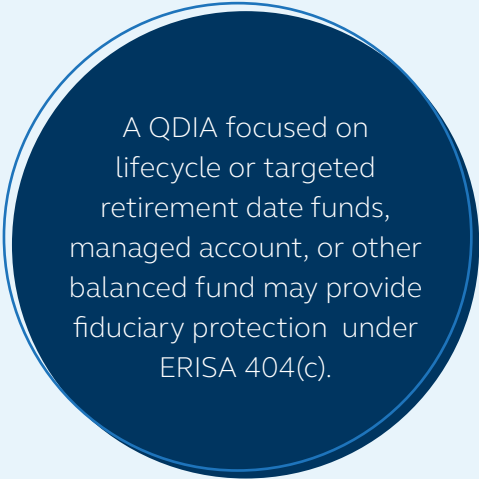
While a written investment policy isn't required, documenting the decision-making process helps fiduciaries meet plan objectives and illustrates guidelines of a prudent decision-making process. Find a sample investment policy statement by using the Help feature on principal.com.

Qualified default investment alternative (QDIA)

Plan sponsors may want to offer a QDIA for participants who fail to make an investment election.

Here's how a QDIA works:

- It's created using one of three long-term investment options that apply generally accepted investment theories.
- It should be diversified to minimize risk of large losses.
- It should be designed to provide varying degrees of long-term appreciation and capital preservation through a mix of equity and fixed-income investment options.



A QDIA focused on lifecycle or targeted retirement date funds, managed account, or other balanced fund may provide fiduciary protection under ERISA 404(c).

ERISA 404(c)

Under ERISA 404(c), plan sponsors and fiduciaries can allow participants to control the investment direction of their account balances. If a plan meets the 404(c) requirements, a fiduciary is not generally liable for investment losses attributable to a participant's investment decisions. Fiduciaries do still retain responsibility for losses that result from their selection of imprudent investment options.

Compliance with 404(c) is optional and several requirements must be met. These include:

- Offering a broad range of diversified investment options.
- Allowing participants to transfer among investment options offered.
- Providing participants with sufficient information to make informed investment decisions.
- Making additional information available to participants upon request.

Employee stock ownership plan (ESOP)

For ESOPs, there are additional considerations. For example, managing cash or other investment(s) is a fiduciary function. And there should be a clear investment policy for those assets. In addition, repurchase liability for an ESOP is an important consideration when evaluating investments.

Note: You have an ongoing duty to monitor all plan investments, regardless of when they were selected. There's no statute of limitations under ERISA.

3

Communicate and educate

Participant communication and education are critical to the success of any retirement program. That's why you'll want to spend some time determining your approach.

Education policy statement

While it's not required, plan fiduciaries may use an employee education policy statement to document program goals and accountability. It also provides a baseline for discussing employee education.

A well-designed education policy can help ensure effective and consistent communications and encourage better participant understanding and decisions. It may also lead to greater levels of participation, higher contribution amounts, and better-invested accounts.

Participant investment advice

Plan fiduciaries also have oversight responsibility for investment advice services provided to plan participants.

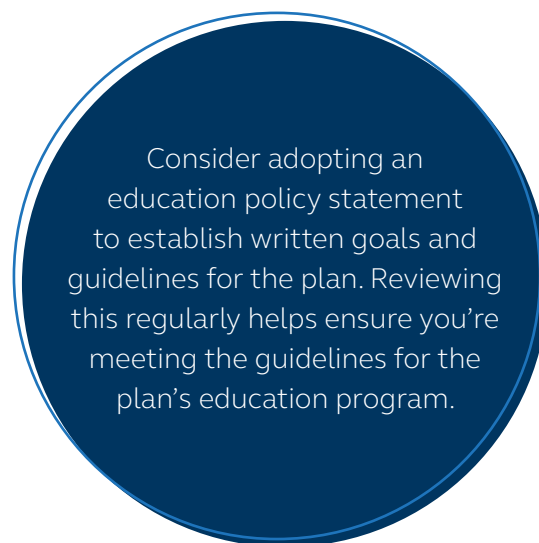
You'll want to know:

1. Is your service provider acting in a fiduciary role to participants?
2. What auditing or verification process do they have in place for the advice service that you may use for monitoring their activities?

It's also important to understand that the safe harbor protection of ERISA 404(c) is limited if participants utilize investment advisory services and haven't maintained control over the investment direction for their retirement plan account.



To make sure your participants get our messages, include their work email addresses when you upload participant data. Not quite sure how to do that? Log in to the employer website and type "email addresses" in the Help feature for step-by-step instructions.



Consider adopting an education policy statement to establish written goals and guidelines for the plan. Reviewing this regularly helps ensure you're meeting the guidelines for the plan's education program.

One aspect of participant communication is investment education. It's important to understand the distinction between investment education and investment advice.

The DOL defines investment education as communication related to:

- Benefits of plan participation
- Basic financial planning strategies
- Calculating retirement income
- Impact of asset allocation on retirement income

While investment education helps guide participants, it cannot give specific answers to participants' investment questions. Under ERISA, providing specific, individualized investment recommendations constitutes investment advice—and persons such as third-party registered investment advisors (RIAs) who provide such advice are considered fiduciaries. Plan fiduciaries should require the selected fiduciary advisor to provide written explanations of their compliance with all necessary requirements.

Automatic plan features

When a defined contribution plan has default investment options, automatic enrollment features, or automatic deferral increase options, it's important for employees to be educated on the plan's design features. As a bonus, this may also give participants a greater appreciation for the plan.

4 Manage prudently

As a plan sponsor you want to make decisions in the best interest of your plan participants. The right plan documentation and procedures will help you reach this goal while managing your plan effectively and prudently.

Timely contributions

If the plan provides for salary deferral contributions, voluntary after-tax contributions, or participant loan payments via payroll deduction, then ERISA and the DOL require the amounts be deposited to the plan as soon as they can reasonably be segregated from the employer's general business assets, but in no event later than the fifteenth business day of the next month. In almost all cases the plan sponsor must deposit the money much earlier because it usually requires only a few days to calculate the amounts and deposit them into the plan.

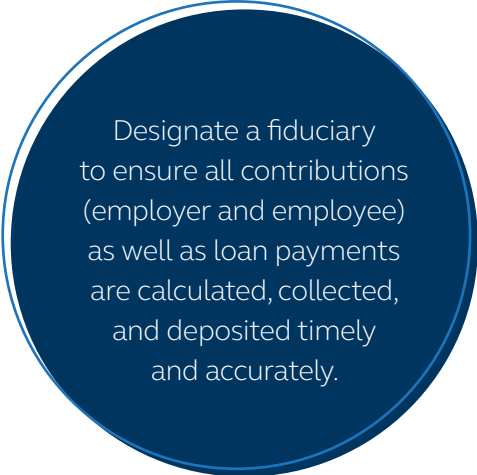
Employer contributions must be calculated according to plan documents and deposited within the IRS standards. Generally, this is no later than the plan sponsor's tax filing deadline.

Note: If your plan has fewer than 100 participants, you may consider the DOL optional safe harbor deposit period. The safe harbor period is seven business days, but it's important to submit amounts sooner if possible.

Plan expenses

It's important to have a full understanding of retirement plan fees and how they're paid. In fact, there's a fiduciary responsibility to monitor the reasonableness of fees and services, including:

- Ensuring the plan operating costs are reasonable compared to the value being received.
- Evaluating services received, quality of services, and overall benefit to participants.



Designate a fiduciary to ensure all contributions (employer and employee) as well as loan payments are calculated, collected, and deposited timely and accurately.

While there's no one right answer, a plan fiduciary should have a repeatable, documented process for evaluating the effect of fees on participants and a rationale for the chosen approach (reasonable fees does not have to mean cheapest). Consider these steps:

1. Gather and evaluate facts, including participant needs.
2. Assess available fee payment methods.
3. Determine the fee collection and documentation process.
4. Provide clear, simple, participant communications.
5. Monitor.

It's a good idea to create and periodically review a fee policy statement. Consider doing this annually and whenever there's a change of financial professional or decision-maker. It's also important to evaluate the total amount paid to all service providers from all sources. And remember to document along the way.

The DOL requires plan service providers to disclose service and fee information—including compensation earned by the service provider and its affiliates. The regulation clarifies the disclosures required to assist a plan fiduciary in evaluating the reasonableness of fees for the services provided.

Plan operations

Plan administrators should also review the plan's operations at least annually to remain familiar with the documented provisions. Items to review may include:

- Employee eligibility and enrollment
- Recordkeeping, including allocations and investment instructions
- Evaluation of the plan service providers
- Vesting of employer contributions
- Withdrawals and distributions
- Annual plan testing
- Participant loans and hardship withdrawals
- Government filings and reporting
- Participant disclosure and communication of plan changes

Prohibited transactions

As a fiduciary you must be aware of what you may not do. Avoid these two general categories of prohibited transactions:

- 1. Interested party** — An interested party is a class of persons or other entity with some tie to the plan, the organization and its owners, the service provider to the plan, the plan participants, or the fiduciary.

One streamlined way to document all the details is by using a fee policy statement. This provides guidelines for the fiduciary to manage plan fees and expenses paid to the service providers. Find a sample fee policy statement by using the Help feature on principal.com.

Certain transactions between the interested party and the plan are prohibited, including:

- Selling, exchanging, or leasing property.
- Extending credit or making loans.
- Providing goods, services, or facilities.
- Transferring or using plan assets for the benefit of the interested party.

- 2. Fiduciary activity** — A fiduciary cannot engage in certain activities, including:

- Using the plan's assets for their own benefit.
- Acting on behalf of someone whose interests are adverse to the plan or its participants.
- Receiving money from anyone dealing with plan assets.

Data security

In April 2021, the Department of Labor (DOL) released **cyber security guidance** for fiduciaries and recordkeepers. Specifically, **Cyber Security Best Practices** and **Tips for Hiring a Service Provider** to assist plan fiduciaries and recordkeepers in their responsibilities to manage cyber security risks.

However, ERISA doesn't spell out exactly what fiduciaries must do related to data security and retirement plans, nor do they mandate a written data security policy. Still, there's one thing the retirement industry does seem to agree on—that a fiduciary should establish a prudent process to thoroughly understand and manage data security risks. The easiest way to show you're following a prudent process is to document that process.

When it comes to documenting a data security policy for retirement plans, there's no one-size-fits-all. Please note that creating any prescriptive document beyond those required by ERISA can carry challenges and risks, so consider focusing on process items rather than laying out any hard and fast rules when documenting data security efforts. And, keep in mind, just as data security risks continue to evolve, so should your risk management strategy.

Fiduciary protection

Managing or administering a retirement plan comes with a lot of responsibility. Make sure you have the right protection in place to cover the individuals who act as plan fiduciaries.

Bonding

Every fiduciary and individual handling plan assets must be bonded according to ERISA unless an exemption applies. Generally, each person must be bonded for at least 10% of the plan assets that he or she handled in the previous year. The bond amount is typically \$1,000-\$500,000, unless the Secretary of Labor requires a larger bond. For plans holding company stock the limit is \$1 million.

Liability insurance

You may also want to consider liability insurance, which generally insures the plan, its fiduciaries, and/or the plan sponsor against losses caused by breach of fiduciary duty. Contact a qualified property and casualty insurance broker or agent to learn more about your options.

Indemnification

Officers and employees who serve as plan officers and employees who serve as plan fiduciaries may expect to be indemnified against liability. An organization can agree to indemnify plan fiduciaries for certain losses that the fiduciary incurs as a result of service. The agreement to indemnify another isn't a fidelity bond or an insurance policy. Any agreement should carefully outline terms and limitations.

Other insurance coverage

A fiduciary liability insurance policy provides the most comprehensive coverage, but some of the following insurance policies may offer some protection.

- **Employee benefits liability (EBL) endorsement to commercial general liability and property insurance** — Mainly covers errors in plan administration, but not breaches of fiduciary duty.
- **Commercial crime policy** — Can satisfy the ERISA bonding requirements, but coverage is usually not as broad. When using this policy to satisfy ERISA, make sure coverage is comprehensive enough to comply with the law. In addition, these policies tend to have “manifest intent” provisions (fidelity bonds don't) that may limit coverage to only intentional and wrongful acts.
- **Cyber security insurance** — While cyber security threats cannot be entirely prevented, measures can be taken to mitigate the risk.

If you take a look at other policies you may have in place, you'll find the following almost always exclude ERISA fiduciary liability insurance:

- Professional liability insurance
- Employer practices liability insurance
- Directors and officers insurance

We're here to help

You have a lot of responsibility, but it doesn't need to be a daunting task. We have a number of resources available to you on the employer website at principal.com. If you want to access the annual fiduciary file, log in and select one of your contracts. In the **Help** feature, search for “Fiduciary File.” It will be the top result.

And be sure to rely on your financial professionals, TPAs, attorneys, accountants, and other professionals to help you manage and navigate your role.



principal.com

The subject matter in this communication is educational only and provided with the understanding that Principal® is not rendering legal, accounting, investment or tax advice. You should consult with appropriate counsel, financial professionals, and other advisors on all matters pertaining to legal, tax, investment or accounting obligations and requirements.

Insurance products and plan administrative services provided through Principal Life Insurance Company®, a member of the Principal Financial Group® Des Moines, IA 50392.

Principal®, Principal Financial Group® and Principal and the logomark design are registered trademarks of Principal Financial Services, Inc., a Principal Financial Group company, in the United States and are trademarks and service marks of Principal Financial Services, Inc., in various countries around the world.

PQ8241-17 | © 2024 Principal Financial Services, Inc. | 3412306-022024 | 02/2024