Preventive Measure:

Self-Audits Help Your Plan Stay in Compliance

by | **Amy Pocino Kelly, Dan R. Salemi** and **Rachel Mann**

Self-audits can help employee benefit plans avoid potential fines and costly corrections while also ensuring that they are paying benefits in accordance with their governing documents. These audits may be more attractive to plans following the passage of SECURE 2.0, which contains provisions that incentivize retirement plans to identify and correct errors.

Due to a significant increase in government agency investigations of plans in recent years, a growing number of employee benefit plan sponsors and boards of trustees are interested in conducting internal compliance self-audits, primarily to ensure that any governmental agency audits of their plans go smoothly.

Although many plans are required to obtain an annual financial statement audit opinion, the financial statement audit process in many cases will not include the fulsome operational review that would be needed to ensure that the plan is consistently operating in compliance with applicable law or the plan's own governing documents.

A preemptive self-audit can help plans identify and correct compliance or operational errors before they are discovered by an agency, such as the U.S. Department of Labor (DOL) or Internal Revenue Service (IRS), during an agency audit. Self-audits also can ensure that plans are paying benefits in accordance with their governing documents. Plans that conduct such audits may avoid large agency fines and overpayments as well as corrections processes that may require agency input and approval.

benefits MAGAZINE

Reproduced with permission from *Benefits Magazine,* Volume 62, No. 2, March/April 2025, pages 16-21, published by the International Foundation of Employee Benefit Plans (www.ifebp.org), Brookfield, Wis. All rights reserved. Statements or opinions expressed in this article are those of the author and do not necessarily represent the views or positions of the International Foundation, its officers, directors or staff. No further transmission or electronic distribution of this material is permitted.

This article will discuss the self-audit process and identify common areas of compliance that plans should target. It will also highlight changes affecting self-audits that are included in the SECURE 2.0 Act of 2022, a package of retirement plan legislation.

What Is a Self-Audit?

A *self-audit* is generally a review of the plan's operational practices against current versions of the written plan document. A self-audit like this is typically designed at the outset to focus on specific operational practices. Once the audit scope is defined, those responsible for conducting the audit will generally work with the plan's administrator to review the in-scope operational practices against the governing plan document provisions and applicable law. They will work to either confirm that such practices are consistent with the plan's terms and applicable law or identify compliance gaps that should be reviewed and potentially corrected. It is a good practice to consider conducting a focused self-audit whenever an operational error is discovered in the routine course of plan administration. In addition, plans should consider a broader self-audit every few years, particularly after there has been a change in a key plan administrator vendor, such as a new third-party administrator (TPA).

Self-audits can help plans and their fiduciaries avoid costly corrections and allegations of breach of fiduciary duties. Sections 402(a)(1) and 404(a)(1)(d) of the Employee Retirement Income Security Act (ERISA) require every employee benefit plan to be established and maintained pursuant to a written instrument and administered according to its written terms. Establishing the plan is a nonfiduciary settlor activity, but the plan's fiduciaries have a fiduciary duty under ERISA to follow the written plan document while managing and administering the plan. Failure to follow the written terms of the plan creates a potential breach of fiduciary duty.

If they don't conduct such self-audits, many boards of trustees and plan administrators may not have appropriate familiarity with the plan terms or certainty that the plan's administrative practices are consistent with the plan terms. This could result in ongoing errors and potential fiduciary breaches that could continue for days, weeks, months or even years if not addressed.

Who Should Conduct a Self-Audit?

Although the method of conducting a self-audit may depend on the type of plan involved, the most effective self-audits are typically conducted with assistance from a consultant, legal counsel or combination of the two. They are often in a better position to objectively evaluate whether the plan's administrative practices comply with applicable law and governing plan documents.

Outside counsel or third-party benefits consultants can also bring deep industry knowledge and broad perspectives to the self-audit and government agency audit process. These types of benefits professionals are more likely to have experience with many types of audits by different government agencies and to have intimate knowledge of the particular audit trends and priorities of the auditors. In addition, they should have experience correcting a wide range of errors and should know the appropriate prospective and retroactive correction options that are available, should errors be discovered. Outside counsel and consultants are also more likely, as compared with the plan's internal staff, to be objective and lack any inherent bias when identifying existing errors and determining whether a particular administrative practice is consistent with the plan's governing documents.

Attorney-Client Privilege

Privilege is one of the benefits of engaging legal counsel when conducting a self-audit, although it is limited as described below.

takeaways

- Self-audits can help employee benefit plans identify and correct compliance or operational errors before they are discovered by an agency, such as the Department of Labor (DOL) or Internal Revenue Service (IRS). Self-audits also can ensure that plans are paying benefits in accordance with their governing documents.
- Regular self-audits review the plan's operational practices against current versions of the written plan document. They may be conducted with assistance from a consultant, legal counsel or combination of the two.
- Self-audits may be more attractive to plans following the passage of the SECURE 2.0 Act of 2022, which contains provisions that incentivize benefit plans to act quickly to identify any previously undiscovered errors and correct them as soon as possible.
- Common areas of focus in recent retirement plan audits by the DOL and IRS include benefit calculations, procedures for finding missing participants and cybersecurity.

Work product that is created during a self-audit, including reports, memos, presentations and emails, is not generally protected by any sort of privilege. Merely including outside counsel on the self-audit team or including outside counsel on emails does not cause the work product to become protected from discovery through attorney-client privilege.

The discovery of any nonprivileged work product that discloses area of risk for a board of trustees and the plan(s) it oversees can be a gold mine for a government investigator or plaintiff's attorney and a land mine for trustees.

When a self-audit is directed by counsel and is done in anticipation of or in preparation for a governmental investigation or litigation, the attorney-client privilege will typically attach to that work product. The ability to protect self-audit work product from damaging discovery is a significant incentive to perform a self-audit at the direction of legal counsel who are engaged to help prepare for a potential or hypothetical government audit or litigation.

Four Sample Issues/Areas for Self-Audit for Retirement Plan Sponsors

These four questions represent common areas of focus in recent retirement plan audits by the Department of Labor (DOL) and Internal Revenue Service (IRS).

1. Is the plan staff or the plan's third-party administrator calculating benefit (e.g., pension) payments and offering the appropriate distribution options and pension commencement date to participants in accordance with the terms of the plan?
2. Primarily in the case of a defined contribution plan, what is the plan's definition of "compensation" and do the contributing employers follow that definition when making contributions?
3. Does the plan have a sufficiently prudent process for identifying and locating missing participants?
4. Does the plan have sufficiently prudent cybersecurity protections to protect plan assets from cybertheft?

SECURE 2.0 Expands the Use of the IRS Self-Correction Program

Self-audits may be more attractive to retirement plans following the passage of SECURE 2.0, which contains provisions that incentivize retirement plans to act quickly to identify any previously undiscovered errors and correct them as quickly as possible.

SECURE 2.0 significantly expands the ability of retirement plan sponsors to "self-correct" certain failures that may arise in day-to-day plan operation and administration. The IRS maintains the Employee Plans Compliance Resolution System, which includes a Self-Correction Program (SCP) through which retirement plan sponsors can self-correct certain types of errors without making a submission to the IRS or obtaining IRS approval. Before SECURE 2.0 was passed, the SCP was available only for limited operational and plan document errors.

SECURE 2.0 expands the scope of operational and plan document errors that can be self-corrected and allows retirement plans to self-correct any "eligible inadvertent failure" to comply with applicable requirements of the Internal Revenue Code (the Code). An *eligible inadvertent failure* is defined as any failure that occurs despite the existence of practices and procedures that are reasonably designed to promote and facilitate compliance with applicable requirements of the Code. However, eligible inadvertent failures do not include any failure that is egregious, relates to the diversion or misuse of plan assets, or is related (directly or indirectly) to an abusive tax-avoidance transaction.

The opportunity to self-correct eligible inadvertent failures is available unless (1) the IRS identifies the failure before any self-correction actions are initiated or implemented, or (2) the self-correction was not corrected within a "reasonable" period after the failure was identified. There is no hard deadline to correct eligible inadvertent failures, provided that the failure is corrected before it is identified by the IRS and within a reasonable period after it is discovered. The IRS has stated that a "reasonable period" is determined by considering all relevant facts and circumstances, and that, in most cases, a correction within 18 months of identification of the error would be considered reasonable.

These two SCP limitations demonstrate the importance of identifying errors early. If an error is identified within a "reasonable" period—and prior to an IRS audit—it may be corrected through SCP without IRS approval. Early identification and prompt correction can save plans and their fiduciaries significant time and money by allowing them

to bypass official corrections programs that require agency oversight. See page 58 for additional information about self-correction procedures available through the DOL's Voluntary Fiduciary Correction Program.

SECURE 2.0 Institutes New Deadlines for Overpayments

Other provisions of SECURE 2.0 provide relief and establish new rules regarding the correction of overpayments from retirement plans, further demonstrating the importance of identifying and correcting pension/retirement benefit payment errors as soon as possible.

Retirement plan overpayments generally include payments that a participant receives that exceed what is permitted under plan terms or applicable regulatory limits. Overpayments may include amounts that a participant is not entitled to receive under the terms of the plan (e.g., incorrectly calculated pension benefits) or amounts that a participant receives prematurely (e.g., impermissible in-service distribution of amounts from a 401(k) plan).

SECURE 2.0 provides that a retirement plan fiduciary will not be considered to have breached its ERISA fiduciary duties if the fiduciary exercises discretion to not seek recovery of an overpayment. If, however, a plan fiduciary does decide to recoup overpayments, SECURE 2.0 establishes rules and limits on how this recoupment effort can be undertaken.

One new overpayment rule from SECURE 2.0 provides that a fiduciary may not seek to recover past overpayments from a participant or beneficiary if the first overpayment occurred more than three years before the participant or beneficiary was first notified of the error in writing. Similar to the new SCP rules, this overpayment rule incentivizes fiduciaries to self-audit plans regularly since the faster a plan identifies overpayments, the more likely it will be able to recoup those overpayments. If the plan fails to identify the overpayment and notify the participant/beneficiary in time and therefore misses the three-year deadline, the plan will no longer be able to recoup the overpayment.

Government Audit Trends and Priorities

Below is a list of some common areas of focus in recent retirement plan audits by the DOL and IRS.

- Is the plan staff or the plan's TPA calculating benefit (e.g., pension) payments and offering the appropriate distribution options and pension commencement date to participants in accordance with the terms of the plan? This is an area of plan document compliance that is often overlooked, in many cases because the plan's benefit calculation and commencement/application processes are not regularly reviewed for compliance with both the current plan document and applicable law.
- Primarily in the case of a defined contribution plan, what is the plan's definition of "compensation" and do the contributing employers follow that definition when making contributions? Possible corrections include:
  - –Amending the plan's definition of compensation to align with the contribution practices of contributing employers or ensuring that contributing employers are making deferral and/or employer contributions in accordance with the plan's current definition of compensation
  - –Determining whether contributions should be refunded for amounts that were improperly included or retroactively amend the plan to match the definition of compensation to the plan's operation in practice. Note that retroactive amendment via an SCP may be available, depending on the circumstances (as discussed above).
- Does the plan's summary plan description (SPD) accurately identify the plan's administrator and fiduciary/fiduciaries? Possible corrections include:
  - –Amending and redistributing an updated SPD to include required information
  - –Investigating whether any specific operational errors were caused by a lack of communication between the participants and plan administrator/fiduciary/fiduciaries, including errors related to the claims and appeals or beneficiary designation processes.

learn more

Education

DOL Developments for Retirement Plans
On-Demand Webcast
Visit *www.ifebp.org/webcasts* for more information.

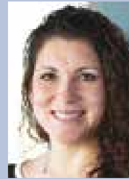
ERISA
E-Learning Course
Visit *www.ifebp.org/elearning* for more details.

- Does the plan have a sufficiently prudent process for identifying and locating missing participants? Possible corrections include:
  –Maintaining (and regularly updating) accurate census information for all plan participants, both current and retired/terminated
  –Coordinating with the recordkeeper to quickly flag missing participants through returned or uncashed checks, bounced emails, etc.
  –Checking related plan or other company records for additional methods of communication for the participant or next of kin, as well as communicating with beneficiaries or other participant contacts for updated contact information.
- Does the plan have sufficiently prudent cybersecurity protections to protect plan assets from cybertheft? Possible corrections include:
  –Coordinating with the plan's recordkeeper and other third-party service providers to ensure that they are complying with the DOL's cybersecurity guidance
  –Reviewing contracts with third-party providers or engaging in a request for information with existing providers to ensure cybersecurity contractual provisions and operations are robust
  –Updating participant communications and/or conducting participant training to inform participants on cybersecurity steps they can take to ensure safekeeping of their assets, such as safe storage of passwords and regular monitoring of online accounts.

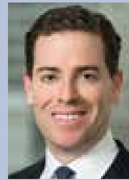
Conclusion

The prospect of a random or targeted government investigation of pension, retirement, and health and welfare plans is daunting. The best way to prepare for a potential investigation is to conduct regular self-audits to help ensure that the plan's operation is consistent with its governing documents and applicable laws. Plans and their boards of trustees should therefore strongly consider conducting regular self-audits to ensure that any governmental investigation of the plan goes smoothly.

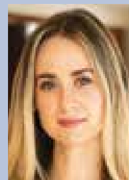
bios



Amy Pocino Kelly is the deputy practice leader for the employee benefits and executive compensation practice at Morgan, Lewis & Bockius LLP. She counsels clients on the design, governance, operation and compliance of qualified and nonqualified retirement plans, equity and executive compensation arrangements, and welfare benefit plans. Pocino Kelly also represents plan sponsors in audit and correction matters before the Department of Labor and Internal Revenue Service. She can be reached at amy.kelly@morganlewis.com.



Dan R. Salemi is a partner in the employee benefits and executive compensation practice at Morgan, Lewis & Bockius LLP and co-chair of the firm's multiemployer plan group. He counsels clients of all types with respect to pension and other retirement plans, health and welfare plans, benefit plan investments, and deferred and equity-based compensation arrangements. Salemi can be reached at dan.salemi@morganlewis.com.



Rachel Mann is an associate in the employee benefits and executive compensation practice at Morgan, Lewis & Bockius LLP. She counsels publicly and privately held companies on employee benefits and executive compensation issues, including complex matters involving Employee Retirement Income Security Act (ERISA) compliance and preemption; qualified retirement, pension, and health and welfare plans; equity and incentive compensation; and employment, retention and severance arrangements. Mann can be reached at rachel.mann@morganlewis.com.

pdf/325