



STATE OF WISCONSIN
Department of Employee Trust Funds
A. John Voelker
SECRETARY

Wisconsin Department
of Employee Trust Funds
PO Box 7931
Madison WI 53707-7931
1-877-533-5020 (toll free)
Fax 608-267-4549
etf.wi.gov

Correspondence Memorandum

Date: August 15, 2022
To: Audit Committee
From: Shellee Bauknecht, Auditor
Office of Internal Audit (OIA)
Subject: Annual Third-Party Administrator (TPA) System and Organization Controls (SOC) 1 Report Review for Calendar Year (CY) 2021

This memo is for Audit Committee review and discussion. No action is required.

This memo provides an overview of the TPA SOC report review for CY 2021. The SOC report review is a component of the Department of Employee Trust Fund's (ETF) TPA oversight procedures. In carrying out its responsibilities under the International Standards for the Professional Practice of Internal Auditing¹, OIA has an ongoing consulting engagement for TPA oversight as part of the FY 2022 – FY 2023 Internal Audit Plan.

Overview of SOC Reporting

SOC reports are issued by independent auditors to attest to the service organization management description of systems and controls that are present and identified. SOC reports can be useful for user entities to understand service organization control objectives and exceptions and to understand a service organization's use and monitoring of its subservice organizations. Reviewing a SOC report can help a user entity identify risk that it may be exposed to and determine whether additional steps

¹ Standard 2050 – Coordination and Reliance: The chief audit executive should share information, coordinate activities, and consider relying upon the work of other internal and external assurance and consulting service providers to ensure proper coverage and minimize duplication of efforts.

Standard 2110 – Governance: The internal audit activity must assess and make appropriate recommendations to improve the organization's governance processes for coordinating the activities of, and communicating information among, the board, external and internal auditors, other assurance providers, and management.

Reviewed and approved by Yikchau Sze, Director, Office of Internal Audit
Electronically Signed 8/31/22

Board	Mtg Date	Item #
AUD	9.22.22	4

should be taken to reduce risk. SOC reports also identify user controls that should be considered by the user entity to achieve control objectives at the service organization.

There are several types of SOC reports which are further described in Attachment A.

SOC reports are not intended to identify controls that are missing or that have not been identified by the service organization. Therefore, ETF also uses contract compliance audits to assess whether controls are adequate to ensure transactions processed for ETF benefit programs are properly executed, recorded, and safeguarded.

ETF SOC Report Review Responsibilities

ETF contracts with various TPAs to administer certain benefit programs or portions thereof, and with vendors for the provision of other direct and supportive services to ETF programs. ETF program managers have the day-to-day responsibility of TPA oversight and the ongoing management and operation of benefit programs and contracted services, including annually obtaining and reviewing TPA SOC reports.

As part of the TPA SOC report review, ETF program managers assess user controls, the use of subservice organizations, and exceptions to control testing. ETF program managers may follow up with TPAs as needed to understand information provided in the SOC reports and its impacts on ETF programs. Additionally, ETF program managers obtain bridge letters for any reports that do not cover the entire calendar year.

OIA facilitates the annual SOC 1 Type 2 report review by engaging and training ETF program managers in understanding SOC reports and assisting in areas that may require additional understanding, including the user controls, subservice organizations, and exceptions to control testing. OIA may also make changes to the SOC 1 Type 2 review process from the prior year to continue improving the review. ETF's Bureau of Information Security Management (BISM) staff are responsible for facilitating the review of SOC 2 Type 2 reports or other mutually agreed-upon security documentation due to their responsibility of ensuring information security at ETF.

CY 2021 SOC 1 Type 2 Report Review

The review of SOC 1 Type 2 reports for TPAs covering CY 2021 began in March 2022 and was completed in June 2022. The review included the following TPAs:

- Optum Financial (Employee Reimbursement Accounts, Health Savings Accounts, and Commuter Benefits Accounts)
- Navitus (Pharmacy Benefit)
- Securian/Minnesota Life (Life Insurance)
- Delta Dental (Uniform Dental Benefit)
- The Hartford (Income Continuation Insurance)
- Empower Retirement (Wisconsin Deferred Compensation)

During the review, several control testing exceptions were noted and one TPA SOC report included a qualified opinion. However, these exceptions, including the deficiency that resulted in the qualified opinion, did not have a significant and adverse impact on ETF programs. Improvements made to ETF's review process included expanding the assessment of subservice organizations to provide additional assurances over TPA subservice organization controls. Some improvements were also made to communicate certain user controls to participating employers, and additional communication is planned to provide guidance to payroll centers on certain user controls.

Attachment A: SOC Report Types



STATE OF WISCONSIN
Department of Employee Trust Funds
 A. John Voelker
 SECRETARY

Wisconsin Department
 of Employee Trust Funds
 PO Box 7931
 Madison WI 53707-7931
 1-877-533-5020 (toll free)
 Fax 608-267-4549
etf.wi.gov

Attachment A

SOC Report Types

Table 1

Report Name	Report Focus	Importance	Users
SOC 1	Control objectives and control activities relevant to the internal controls over financial reporting.	Impact financial statements	<ul style="list-style-type: none"> • Management of service organization • User entities and auditors
SOC 2	System controls related to security, availability, processing integrity, confidentiality and/or privacy.	<ul style="list-style-type: none"> • Governance, risk and compliance programs • Oversight • Due Diligence 	<ul style="list-style-type: none"> • Management of service organization • User entities and auditors

Table 2

Type 1	Type 2
Describes the design of the system (policies and procedures).	Describes the design of the system and provides the <u>testing</u> results on the effectiveness of controls.
CPA's opinion on the fairness of management's description and the suitability of system and control design at a <u>point in time</u> .	CPA's opinion on the fairness of management's description, the suitability of system and control design, and <u>operating effectiveness of controls</u> for a period of time.