Texas County & District Retirement System

System and Organization Controls (SOC 1SM) Report on Texas County & District Retirement System's Description of its Pension Management System and the Suitability of the Design and Operating Effectiveness of Controls

For the Period May 1, 2023 to April 30, 2024

The SOC1 Report is intended for TCDRS participating employers and their auditors. The SOC1 Report contains critical TCDRS infrastructure information, which is confidential under state law. This report or portions of this report may not be released to the public without the express permission of TCDRS.

Texas County & District Retirement System

System and Organization Controls (SOC 1[SM]) Report

Pension Management System

For the Period May 1, 2023 to April 30, 2024

Table of Contents

Section I.

Independent Service Auditors' Report Provided by KPMG LLP

KPMG LLP
1601 Market Street
Philadelphia, PA 19103-2499

Independent Service Auditors' Report

To the Board of Trustees of the Texas County & District Retirement System:

Scope

We have examined management of Texas County & District Retirement's (TCDRS) accompanying description of its Pension Management system (the System) for processing user entities' transactions throughout the period May 1, 2023 to April 30, 2024 titled "Management of Texas County & District Retirement System's Description of its Pension Management System" (the Description) and the suitability of the design and operating effectiveness of the controls included in the Description to achieve the related control objectives stated in the Description, based on the criteria identified in "Management of Texas County & District Retirement System's Assertion" (the Assertion). The controls and control objectives included in the Description are those that management of TCDRS believes are likely to be relevant to user entities' internal control over financial reporting, and the Description does not include those aspects of the System that are not likely to be relevant to user entities' internal control over financial reporting.

TCDRS uses subservice organizations identified in Section III to perform some of the services provided to user entities that are likely to be relevant to those user entities' internal control over financial reporting. The Description includes only the control objectives and related controls of TCDRS and excludes the control objectives and related controls of the subservice organizations. The Description also indicates that certain control objectives specified by TCDRS can be achieved only if complementary subservice organization controls assumed in the design of TCDRS's controls are suitably designed and operating effectively, along with the related controls at TCDRS. Our examination did not extend to controls of the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of TCDRS's controls are suitably designed and operating effectively, along with related controls at TCDRS. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In Section II, management of TCDRS has provided the Assertion about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description. TCDRS is responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion, providing the services covered by the Description, specifying the control objectives and stating them in the Description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the Assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the Description.

KPMG

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in the Assertion, the Description is fairly presented and the controls were suitably designed and operated effectively to achieve the related control objectives stated in the Description throughout the period May 1, 2023 to April 30, 2024. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved
- evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the System that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives stated in the Description, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section IV.

Opinion

In our opinion, in all material respects, based on the criteria described in the Assertion:

- the Description fairly presents the System that was designed and implemented throughout the period May 1, 2023 to April 30, 2024
- the controls related to the control objectives stated in the Description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period May 1, 2023 to April 30, 2024, and subservice organizations and user entities applied

the complementary controls assumed in the design of TCDRS's controls throughout the period May 1, 2023 to April 30, 2024

- the controls operated effectively to provide reasonable assurance that the control objectives stated in the Description were achieved throughout the period May 1, 2023 to April 30, 2024 if complementary subservice organization controls and complementary user entity controls, assumed in the design of TCDRS's controls, operated effectively throughout the period May 1, 2023 to April 30, 2024.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of management of TCDRS, user entities of TCDRS's System during some or all of the period May 1, 2023 to April 30, 2024, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

May 31, 2024
Philadelphia, Pennsylvania

Section II.

Management of Texas County & District Retirement System's Assertion

Management of Texas County & District Retirement System's Assertion

We have prepared the accompanying description of Texas County & District Retirement System's Pension Management system (the System) for processing user entities' transactions throughout the period May 1, 2023 to April 30, 2024 titled "Management of Texas County & District Retirement System's Description of Its Pension Management System" (the Description) for user entities of the System during some or all of the period May 1, 2023 to April 30, 2024, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the System themselves, when assessing the risks of material misstatement of user entities' financial statements.

TCDRS uses the subservice organizations identified in Section III, to perform some of the services provided to user entities that are likely to be relevant to those user entities' internal control over financial reporting. The Description includes only the control objectives and related controls of TCDRS and excludes the control objectives and related controls of the subservice organizations. The Description also indicates that certain control objectives specified in the Description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively along with the related controls at TCDRS. The Description does not extend to controls of the subservice organizations.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of TCDRS's controls are suitably designed and operating effectively, along with related controls at TCDRS. The Description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

a) The Description fairly presents the System made available to user entities of the System during some or all of the period May 1, 2023 to April 30, 2024 for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the Description

   i. presents how the System made available to user entities of the System was designed and implemented to process relevant user entity transactions, including, if applicable,

      (1) the types of services provided, including, as appropriate, the classes of transactions processed;

      (2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the System;

      (3) the information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities;

      (4) how the System captures and addresses significant events and conditions other than transactions;

      (5) the process used to prepare reports and other information for user entities;

(6) services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them;

(7) the specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls;

(8) other aspects of our control environment, risk assessment process, information and communication (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

ii. includes relevant details of changes to TCDRS's System during the period covered by the Description.

iii. does not omit or distort information relevant to TCDRS's System, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities of the System and their auditors, and may not, therefore, include every aspect of the System that each individual user entity of the System and its auditor may consider important in its own particular environment.

b) The controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period May 1, 2023 to April 30, 2024 to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of TCDRS's controls throughout the period May 1, 2023 to April 30, 2024. The criteria we used in making this assertion were that:

i. the risks that threaten the achievement of the control objectives stated in the Description have been identified by management of TCDRS;

ii. the controls identified in the Description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved; and

iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Texas County & District Retirement System

May 31, 2024

Section III.

Management of Texas County & District Retirement System's Description of its Pension Management System

Overview of Operations Related to TCDRS

For more than 55 years, the Texas County & District Retirement System (TCDRS) has been a model for providing reliable responsibly funded retirement benefits. TCDRS partners with more than 865 Texas counties and governmental districts to provide retirement, disability and survivor benefits to more than 379,000 Texans. Our benefits help participating employers attract and retain talented staff. In addition, pooled investments and plan administration enable them to benefit from economies of scale.

With TCDRS, employers and employees save for benefits in advance throughout an employee's career. TCDRS pools and invests these funds with the returns compounding over time. As a result, investment earnings fund nearly 74% of every benefit dollar. Our 30-year return is 7.6% for the period ended December 31, 2023.

TCDRS has the following built-in features:

- TCDRS is a savings-based plan. Members save for their retirement over the length of their careers. At retirement, TCDRS benefits are based on a member's final savings balance and employer matching. This unique design makes costs more predictable for our employers.
- TCDRS is a model of responsible funding. The system as a whole is 89% funded. We do not receive funding from the State of Texas. Each plan is funded by our employers, members and investment earnings. Employers participating in the system must pay 100% of their required contributions every year. In addition, TCDRS has one of the most conservative funding policies in the nation. By paying the required contribution rate, employers are paying for their current employees' future benefits and are paying down any unfunded liabilities to zero within 20 years. This helps ensure that funds will be there when employees are ready for retirement.
- TCDRS is not a one-size-fits-all system. Each employer maintains its own customized plan of retirement benefits. In addition, employers have the flexibility and local control to adjust their benefits each year based on their needs and budgets. This level of flexibility is not standard in most traditional pension plans.

TCDRS is administered by a nine-person Board of Trustees appointed by the governor and confirmed by the state senate. The board appoints a director to oversee all day-to-day operations, and a chief investment officer, to oversee investment operations. The board also appoints legal counsel, a consulting actuary, an independent auditor, a medical board and investment consultants.

The TCDRS Board of Trustees uses Policy Governance®, a governance model, to define the purpose and strategic direction of TCDRS. The board establishes TCDRS's mission and strategic goals or desired results, called the Ends, and monitors performance against these policies.

TCDRS key controls and control activities are designed to achieve the organization's control objectives. Control activities are part of the processes TCDRS uses to achieve its business objectives. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed and improved (when necessary) to meet the overall objectives of the organization. Business and information technology processes are built to support established controls and enable TCDRS to achieve objectives consistently.

Relevant Aspects of Control Environment, Risk Assessment Process, Information and Communication and Monitoring

Internal Control Description Using COSO Framework

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) has defined internal control as a process effected by an entity's board, management and other personnel that provides reasonable assurance that the objectives of the entity will be achieved. The COSO internal control standards approach internal control through a hierarchal structure of five components and 17 principles. The five components — control environment, risk assessment, control activities, information and communication, and monitoring — must be effectively designed, implemented and operated together in an integrated manner. The 17 principles represent requirements necessary to establish an effective internal control system. A description of TCDRS's internal control system using the COSO components and principles follows.

Control Environment

The set of standards, processes and structures that provide the basis for carrying out internal control across the organization.

TCDRS demonstrates a commitment to integrity and ethical values. TCDRS has adopted a code of ethics, published on the TCDRS website, which applies to trustees and executive staff. In addition, the TCDRS Employee Handbook contains basic standards of conduct for all staff that emphasize ethical behavior – including explicit prohibitions on bribery and conflicts of interest.

The Board of Trustees demonstrates independence from management and exercises oversight of the development and performance of internal control. The TCDRS Board of Trustees' Policy Manual outlines organizational goals (Ends) that include safeguarding assets. Management is required to report on their compliance with the Ends on an annual basis. Board policies also define activities that the staff should avoid (Executive Limitations). The board monitors adherence to these policies on an annual basis, with some financial activities monitored every quarter. The monitoring processes for the Ends and Executive Limitations require management to provide information demonstrating to the board that the policies are being followed and require the board to assess whether that information shows compliance.

Management establishes structures, reporting lines and appropriate authorities and responsibilities in the pursuit of objectives. The executive director and chief investment officer are each responsible for delegating duties to achieve the organization's strategic goals or Ends. The current organizational structure is provided to all management and staff via the intranet and a high-level org chart is published in the *TCDRS Annual Comprehensive Financial Report*. The organizational structure helps employees understand where they fit into TCDRS overall, from whom to take direction and the scope of their roles.

TCDRS demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. A core component of the current strategic plan is a commitment to strengthen organizational responsiveness. The plan includes specific objectives to continue efforts to develop needed skills in the workforce to manage new technologies and services, and to provide for succession planning. The plan also directs staff to implement the redesigned employee recruitment and onboarding program to help ensure employees are aligned with our values and are provided with the information and support they need to be successful; and to help ensure that employees are respected, supported and valued. TCDRS conducts an annual market analysis of salaries to maintain employee compensation at competitive levels. TCDRS provides adequate resources to help ensure that staff receives education, training and development.

TCDRS holds individuals accountable for their internal control responsibilities in the pursuit of objectives. All TCDRS employees receive an annual performance review, a key component of which is quality of work. In addition to the formal review process, supervisors are also expected to provide ongoing performance feedback. The employee handbook outlines disciplinary actions that may be implemented in the case of poor performance or policy violations.

Risk Assessment

A dynamic and iterative process for identifying and assessing risks to the achievement of objectives.

TCDRS specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. TCDRS maintains a four-year strategic plan that outlines the objectives for the organization. Every two years, management updates the strategic plan to help ensure that priorities are reassessed and risks facing TCDRS are properly considered. Every year an operational plan is created that gives specific goals for the coming year. The most recent strategic plan was finalized in September 2022.

TCDRS identifies risks to achieve its objectives across the entity and analyzes risks to determine how they should be managed. Key risks to the organization are included in ongoing monitoring reports provided to the board. Additionally, the Internal Audit department conducts a risk assessment as part of the annual planning of control reviews. The risks and controls related to key benefit processing areas have been documented and are maintained on the TCDRS intranet.

TCDRS considers the potential for fraud in assessing risks to the achievement of objectives. Financial and data assets are key targets for fraud. Risk assessments relating to management of these assets include the potential for theft or misuse. Management participates in fraud interviews with the external auditor during the audit of financial statements.

TCDRS identifies and assesses changes that could significantly impact the system of internal control. Management reviews risks and internal controls related to process and system changes before implementation. The strategic planning process also requires forward-looking examination of environmental, customer and internal changes that could affect the ability to meet organizational objectives.

Information and Communication

The continual, iterative process of providing, sharing, obtaining and using relevant and quality information from internal and external sources.

Information Technology (IT) controls establish the control environment in which information, applications, network, and operating systems are developed and maintained. The applications that support TCDRS's core business processes include:

- A custom website that uses Optimizely for content management and a Microsoft SQL database.
- Compass, a custom application that leverages the Pega customer service platform and a SQL database, combines workflow and pension processing into a single interface for benefit plan and member demographic information, business rules, workflow management, and orchestrations. Compass also serves as a CRM that allows the TCDRS call center to interact with members and collect benefit application information.
- tEDS, an enterprise SQL Server database serves as TCDRS's system of record for member, retiree, and employer data.
- IBM FileNet as the TCDRS document repository. TCDRS's document scanning software, Kofax, interfaces with FileNet.

- Dynamics Great Plains (“Dynamics GP”) is used to support TCDRS’s financial and human resources functions.
- tERS, a reporting server that contains replicated data from Dynamics GP, Pega, the TCDRS website, and tEDS, is used for SSRS reporting.
- Employer Portal is a secure website that acts as a portal for authorized employer contacts to enroll and manage member information, review and authorize benefit plans, report payroll, and receive reports.
- Member Portal is a secure website that allows members and retirees to access their accounts online, update demographic information, manage accounts and apply for service retirement and withdrawal benefits. Access is secured through a third-party tool, Okta, which enables two-factor authentication. Read-only access for TCDRS staff to an Administrative Portal showing online member activity is also enabled via Okta.
- An authentication process implemented on the website and Compass provides confidence that member transactions remain secure.
- Azure DevOps is used for tracking technical work and releases. SysAid Help Desk is used for documenting requests and approvals related to access management. Privileged Access Management Secret Server manages privileged access and includes workflow approval to manage and monitor access.

The Optimizely, IBM FileNet, Azure DevOps and SysAid Help Desk systems referenced throughout are not included in the scope of this report. Information from those systems is specific to content management or document repositories. None of these systems generate the primary information used for capturing and reporting user entity financial transactions.

TCDRS’s control activities are focused on core systems that support defined control objectives. Although there are other TCDRS systems that support general business processes, these core systems have a direct impact on key controls and control activities that have been designed to achieve the organization’s control objectives.

TCDRS obtains or generates and uses relevant, quality information to support the functioning of internal control. Management and staff in many divisions — including Actuarial Services, Internal Audit, Anti-Fraud, Finance, Human Resources, Information Technology, Legal, Employer Services, Member Services, and Records Management — participate in industry-specific professional associations to maintain current knowledge of regulatory, economic, political and technological changes affecting pension plans.

Connected reporting databases allow management to run ad hoc analyses of processes and data. An enterprise relational SQL pension database (tERS) provides real-time information for processing, and the Compass system includes tools for workflow reporting. A data management review cycle is conducted on a recurring basis to validate system-of-record data that impacts core business processes. A data management program identifies data exceptions that are reviewed and corrected as appropriate to help ensure data remains accurate and reliable.

TCDRS applies several levels of data protection to mitigate losses due to system malfunction, hardware failure, or other sources of data loss or corruption. The TCDRS Infrastructure Services team helps ensure that infrastructures operate in high availability mode to minimize downtime. This includes redundancy for servers, storage and network equipment. In addition, disaster recovery testing is completed annually to help ensure staff and failover procedures are effective and efficient.

TCDRS uses a third-party data center provider, Data Foundry. Their facility provides redundant power and utility services including redundant uninterruptible power supplies and generators, redundant climate control and redundant telecommunication lines. In addition, the facility was constructed to withstand

severe weather and is staffed to enable robust physical security. The scope of this report does not include controls performed by Data Foundry.

TCDRS internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. Internal communication is facilitated through a number of channels, including a weekly internal newsletter (*Trailhead*) and monthly meetings of all division directors. Employee meetings are held regularly within each team and division, and the entire staff meets on a quarterly basis. TCDRS makes extensive use of an intranet to communicate within and across divisions. The intranet homepage includes links to the strategic plan and board policy manual. The intranet also provides access to internal policy and procedures documents, including the TCDRS Employee Handbook and the Information Technology Security Policy.

TCDRS communicates with external parties regarding matters affecting the functioning of internal control. TCDRS receives information from employers through an annual employer survey that includes an assessment of organizational performance and ongoing feedback surveys. In-person visits from field staff and an annual conference for decision-makers and local plan administrators allow for face-to-face discussions with employers. TCDRS also conducts multiple webinars throughout the year to provide information to employers. New administrative contacts at employers are provided one-on-one training via phone and the web. Ongoing satisfaction surveys for key employer and member activities provide the opportunity for customers to communicate with TCDRS about the effectiveness of services offered. Any policy, procedure or process changes that affect customers are communicated through member and employer newsletters (print and electronic) and the TCDRS website. TCDRS also maintains an active social media presence through Facebook and Twitter that provides two-way communication with interested stakeholders.

Monitoring

Ongoing evaluations, separate evaluation or some combination of the two are used to ascertain whether each of the five components of internal control is present and functioning.

TCDRS selects, develops and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. Certain high-risk activities, such as payment processing, are continually monitored through monthly and quarterly performance reporting. Other activities are monitored via email notices to executive management and Internal Audit each time those activities are completed. An annual cross-divisional project team is used to help ensure that income allocation, actuarial valuation and other yearly processes are completed on schedule and in the correct sequence.

The Internal Audit division creates an annual plan to review control activity design and performance. The plan includes both periodic reviews of key processes and ongoing application and network directory access recertification.

A third-party security vendor conducts network penetration testing for both the internal and external network infrastructure. They also perform application testing for the website and the TCDRS pension application, Compass. Website code reviews are also completed as part of this process. Logic Monitor is used for network and performance monitoring for all servers and network infrastructure. Dynatrace is an application monitoring solution used to provide application statistics and monitoring for the TCDRS pension application and the VMWare virtual environments.

Third-party service providers – including JPMorgan, Data Foundry, ThreatMetrix (which is a LexisNexis product that includes Emailage and PhoneFinder), Okta and Plaid – are monitored through review of SOC 1 and SOC 2 reports via a cybersecurity risk program. TCDRS management reviews and certifies that complimentary user entity controls required by those providers have been put in place and reviews any testing exceptions to determine whether those control failures expose TCDRS data or systems.

TCDRS evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the Board of Trustees, as appropriate. Control deficiencies are discussed during regular meetings with management and the director. If necessary, ad hoc cross-departmental meetings are scheduled to discuss issues that require remediation by multiple divisions. The Internal Audit department tracks control change recommendations and provides status updates to the director on a regular basis. Additionally, any control failure that creates an exception to the Ends or Executive Limitation policies is reported to the board either through scheduled monitoring reports or more often if warranted.

Control Activities Overview

The actions established through policies and procedures that help ensure that management's directives to mitigate risk to the achievement of objectives are carried out.

TCDRS designs control activities to achieve objectives and respond to risks. Overall organizational performance is assessed and communicated to key stakeholders via a number of processes, including operational plan development, the "Letter of Transmittal" in the TCDRS Annual Comprehensive Financial Report and monitoring reports to the TCDRS Board of Trustees on the Ends policies. Performance metrics have been established to provide information for these reports. TCDRS management and staff document risks and controls for key processes, such as benefit payment processing and employer and member contribution processing. These risks and controls are documented on a dedicated intranet site and are regularly reviewed by executives, management and staff.

Continuous monitoring of several high-risk payment-related processes provides ongoing reporting of exceptions to management and to the Board of Trustees. Duties for initiating payments and processing contributions are segregated across departments so that no one person or team can send or receive funds on their own. Physical security of the building includes full-time building alarm monitoring, video cameras, security personnel and electronic access security doors that restrict access to certain areas of the building. Access to key information assets stored in databases, on the TCDRS network and with external vendors is managed through an extensive Information Technology Security Policy and is monitored through a comprehensive access recertification process.

TCDRS selects and develops general control activities over technology to support the achievement of objectives. TCDRS's information security program includes a documented security policy that is regularly reviewed and updated. Human resources security practices include security awareness training and background checks. TCDRS has also implemented physical and environmental controls and a comprehensive disaster recovery policy that is reviewed and tested annually. The Information Technology Security Policy includes policies for network security and monitoring, backups and disaster recovery, and an incidence response plan. A documented software release process provides assurance that the changes are first approved by business management and tested by both IT staff and end users before deployment.

TCDRS deploys control activities through policies that establish what is expected and procedures that put policies into action. The TCDRS intranet contains policy and procedure libraries for intra- and cross-divisional use. The TCDRS Employee Handbook includes a reference to a published policy on information resources usage. Both the TCDRS Employee Handbook and this policy are reviewed with all employees. TCDRS also has an access recertification policy to continually review user access to critical applications and data.

Scope/Examination Period

The examination period for the report spans a twelve-month period, from May 1, 2023 to April 30, 2024. The period was selected in order to include controls related to the fiduciary net position of TCDRS as of December 31, 2023. Interest allocations for the Subdivision Accumulation Fund (SAF) and Reserve funds are based on the Board of Trustees' actions taken no later than March following the respective December and therefore are included in this report. The scope of the report includes the general computer controls related to the environment of systems and infrastructure located at TCDRS in Austin, Texas supporting the Dynamics GP, and Compass, applications and databases, Employer Portal and Member Portal applications, and the tERS reporting database.

Pension Trust Fund Accounts

TCDRS pension benefits are funded and paid using separate funds and accounts, each with their own provisions for how balances should be increased or decreased for income allocation and other activity.

- The Employees Saving Fund (ESF) contains an account for each member. Each account is increased as a member makes deposits and interest is allocated. Accounts are reduced for payments due to withdrawal or death, and by retirement. Accounts may also be reduced due to inactivity through transfers to the Endowment Fund. These endowment fund transfers are reversed when the employee claims their benefit so that withdrawal or retirement benefits can be paid. Employee accounts receive a 7% interest rate allocation based on the account's January 1 balance and in accordance with statutory requirements outlined in the TCDRS Act. Individual member ESF accounts are aggregated for each employer and each employer's plan assets include both the aggregate ESF and Subdivision Accumulation Fund (SAF) balances.
- The SAF is used to fund plan benefits and consists of an account for each participating employer. The SAF account is increased as the employer makes contributions. These contributions include both ongoing payroll contributions and additional lump sum employer contributions made through a separate authorization and payment process. When an employee retires, their ESF balance is transferred to the SAF and all retirement benefits are paid from this fund. Annually, the Board of Trustees decides on the income allocation to each participating employer's SAF balance. Employer SAF accounts increase if there is a positive allocation of earnings; accounts decrease in the case of a negative allocation. The Board of Trustees approves an allocation based on investment returns and executive recommendations. The approved allocation is documented in the Board of Trustees' minutes to help ensure allocation complies with the approved rate. For fiscal year 2023, each actively participating subdivision's total assets (the sum of the January 1, 2023 ESF and SAF balances) was multiplied by 2% to determine a total income allocation amount. Each subdivision's SAF allocation is equal to the total income allocation for the subdivision minus the 2023 ESF allocation for that subdivision.
- The Endowment Fund includes contingency reserves that help keep employer contribution rates stable and offset the potential of an adverse investment experience. Inactive accounts transferred from the ESF and reserves to transfer to the Expense Fund for the upcoming year's operating expenses are also included. The Finance team calculates available income (or loss) to allocate to general reserves based on investment income remaining after income allocation to the other funds.
- The Income Fund includes net investment results (income or loss), which are allocated to funds per the TCDRS Act. Any remaining excess or shortage is transferred to or from the Endowment Fund.

Business Process Controls

Census Reports and Accounting Valuation Process

Control Objective 1: Controls provide reasonable assurance that reporting of participant census and accounting valuation data to the TCDRS outside actuary is complete and accurate.

Member Enrollment and Demographic Data

Member enrollment is initiated by authorized employer personnel. TCDRS portal user roles authorized to enroll new employees include Security Administrator, Benefits Administrator, and Payroll Administrator. TCDRS conducts regularly scheduled webinars and seminars to provide information regarding member eligibility and the enrollment process. Additional guidance for enrollment eligibility is posted on the TCDRS website and provided in the TCDRS Administrator Handbook. TCDRS internal processors are restricted from entering or modifying new member information. Instead, new member enrollment data is systematically integrated from authorized employer entry or file upload using the website's secure Employer Portal to the TCDRS pension system, referred to as Compass.

The TCDRS website validates key new member data using Social Security number and birthdate prior to uploading the information to confirm that the data provided is reasonable. All exceptions must be corrected by the employer prior to the website completing the upload process. Compass enforces valid date of birth entries for new members. Once the upload of enrollment data is complete, the website will provide enrollment confirmation to the employer. Authorized employer representatives can confirm all enrolled members through Employer Portal activity. This information provides assurance that the data uploaded was correctly received by TCDRS. Additionally, a monthly New Member Listing, generated from the system of record database, is posted to a secure TCDRS Employer Portal for authorized employer personnel to verify new member demographic information. TCDRS portal user roles authorized to view reports include Security Administrator, Benefits Administrator, Payroll Administrator, and Decision Maker. The report provides assurance that all new members were correctly enrolled. Members also have an opportunity to validate their demographic information through an annual account statement published to the Member Portal and by viewing their information online.

Authorized employer representatives (Security Administrator, Benefits Administrator, and Payroll Administrator) resolve any identified issues with new member data and maintain date of birth data for existing members so that the process remains controlled and aligned with employers' human resources records. A verified contribution and member account are required to finalize a new TCDRS membership in compliance with TCDRS policy.

Benefit Plan Provisions

All authorized annual benefit plan changes are conducted in compliance with the TCDRS Act. Employers can evaluate various benefit plan scenarios and each proposed plan's impact on cost and funding using TCDRS's Plan Customizer secure website tool. Plan changes are initiated by an authorized Decision Maker or Security Administrator's submittal of an elected plan through the secure Employer Portal on the TCDRS website. Submittals automatically generate an internal Compass system case that follows a controlled workflow, including a required verification step by separate Employer Services and Employer Plan Management team members to help ensure plan changes are authorized and accurately updated.

All benefit plan changes require a Plan Agreement to be executed by authorized employer decision-makers. TCDRS Employer Services staff compares the plan document signatory with the TCDRS employer portal to confirm the document was executed by an authorized employer representative. Plan provisions submitted and associated documentation are also reviewed by authorized Employer Plan Management staff to confirm that changes comply with statutory requirements and all documentation is complete. Confirmation of documents received, and plan changes submitted are conducted through a case-reconciliation process using separate website and pension system information.

TCDRS also initiates multiple, plan-related communications to confirm that all provision information has been received and accurately processed. Employer-based communications are generated to verify that all desired plan changes have been submitted as part of the annual plan decision-making process. Confirmations of plan changes are also sent to the employer as a final review step. Benefit plan information is posted to the TCDRS website annually for employer verification.

Completion of all plan provision data verification steps is required prior to generating the plan data file for the consulting actuary as part of the actuarial valuation process. All plan data captured in the file is verified using a system generated plan change report, new employers are confirmed as being included in the file, and all altered employer participation statuses are also reviewed. The Information Technology team confirms the completeness of the file along with conducting a general data review. The TCDRS Actuarial Services team conducts a detailed review of all employer and benefit plan data included in the plan file using the Compass pension system and website plan submittal data as the basis.

Actuarial Valuations Process

An actuarial valuation process performed by an independent consulting actuary generates both funding and accounting valuation results. Separate actuarial review and calculation processes help ensure valuation controls are achieved. The TCDRS Actuarial Services team reviews and confirms source data by comparing valuation file data to the verified Compass system and prior year valuation data.

An independent consulting actuary, selected by the Board of Trustees, calculates and certifies valuation results for the system and for each participating employer. The consulting actuary performs calculations and reviews and certifies valuation results as needed related to changes in benefit plan provisions and additional employer funding in accordance with actuarial principles and standards of practice.

An independent auditing actuary, also selected by the Board of Trustees, performs an alternating replication audit and peer review audit of the valuation process every four years to help ensure that actuarial methods and assumptions are reasonable, the valuation results are determined correctly, and that all components of the valuation process comply with actuarial principles and standards of practice. An actuarial audit report is generated, presented and reviewed by TCDRS executives and the Board of Trustees as part of this audit process.

Generating Member and Retiree Actuarial Valuation Data

Separation of functions and different verification steps performed by the Employer Services, Finance, Information Technology, and Actuarial Services teams creates assurance in the valuation file process. Data verification is completed at the point of entry, and also prior and subsequent to generating the member and retiree valuation files.

Member demographic data, payroll contribution reports, deposit transactions, service credit, account balances, transaction effective dates, and account statuses are confirmed by Employer Services using multiple system reports prior to generating the actuarial valuation file. The reports include:

- Duplicate Member report
- Employer Threshold report
- ESF Transactions report - ESF Details by Transaction Type
- Account Balance Exceptions report
- No Employer Deposits by Month report
- Accounts Created within 1 Month of Termination report
- Employer Payroll Submissions report

The Finance team balances the Employees Saving Fund using two separate systems. The pension SQL database contains all member account balance and transaction information while Dynamics GP contains the summary employee and detailed employer fund data. Both systems track financial transactions separately and are balanced prior to generating the valuation file. Employee transactions reflected in the monthly Compass integration journal entries are reconciled between Dynamics GP and Compass prior to posting to help ensure account changes are accurate. The Finance team reviews the balances monthly via the “3XXXX” fund balancing to confirm data accuracy, with exceptions resolved prior to forwarding the actuarial valuation files, to the consulting actuary for calculations.

Information Technology (IT) generates the valuation files at the request of the Employer Services team. IT verifies the member and retiree valuation file for completeness by generating separate queries from the source system and the valuation file. Any exceptions are identified and resolved prior to forwarding the file to Actuarial Services for data verification. The member valuation file contains active members and inactive members that are entitled to, but not receiving benefits. Employment termination dates posted to a member’s account, without a retirement or withdrawal application processed for that member, would result in the reclassification of the member’s status from active to inactive. The retiree valuation file contains inactive members who have begun receiving retirement benefits.

Actuarial Services reconciles the member and retiree data included in the valuation files based on summarized amounts and counts, and a detailed review of expected data on both the employer level and the individual member level. The confirmed valuation files are used by the consulting actuary to perform funding and accounting calculations. The consulting actuary also receives information on fund balances and cash flows.

Receiving Valuation Data

The Actuarial Services team reviews the funding and accounting valuation results received from the consulting actuary. Plan asset and benefit plan provision information is checked for each employer to help ensure it is identical to the information sent to the consulting actuary. Member and retiree counts for each employer are also reviewed to help ensure they are consistent with the data provided to the consulting actuary. Additional review of the results is also completed that includes the following in addition to other data verification steps: elected rates with benefit plan options, changes in employer contribution rates, and employee and employer fund balances. Unexpected changes in employer liabilities are reviewed by the consulting actuary. The confirmed employer valuation data and documentation results are reviewed for reasonableness and consistency by Actuarial Services and the consulting actuary.

IT follows deployment procedures to load valuation data into tables accessible by Compass systems. Approved valuation data results are loaded in each system environment: development, integration, user acceptance testing and production. After the data is loaded, it is reviewed by Actuarial Services for completeness and accuracy. Final approval by the consulting actuary of the Plan Customizer (which uses the valuation data loaded into the pension system) is also required in the production environment prior to use. Certified valuation reports are loaded to the secure TCDRS website for access by authorized employer contacts.

Contributions

Control Objective 2: Controls provide reasonable assurance that contributions received from employers are completely and accurately posted to the employee and employer accounts.

Contribution Rates

Employers submit employee payroll deposit reports, any reporting adjustments, and contributions on a monthly basis. Contribution amounts are based on a plan authorized employee deposit rate and an actuarially determined employer contribution rate necessary to fund plan benefits (or a higher rate elected by the employer). Employee compensation serves as the basis for employee and employer contributions. Employer guidance on compensation that is used in the contribution calculation is posted on the TCDRS website, available in the TCDRS Act, and included in the *TCDRS Handbook for Administrators*. In addition, TCDRS provides on-demand training via webinar for payroll administrators.

Employer contribution rates are annually determined by the consulting actuary as part of the funding valuation process and are based on a combination of plan experience, actuarial assumptions, and authorized benefit plan provisions. Plan-based employer contribution rates are communicated to employers prior to the new reporting year. TCDRS sends an email communication containing new employer contribution rates to each employer as a reminder to use updated rates for the new plan year. Contribution rates are also posted on the secure TCDRS website for authorized employer access and confirmation. The Employer Threshold report from the Dynamics GP accounting system confirms the correct employer contribution rates are used by the employer based on reported monthly employee contributions and current contribution rates. All reported contribution amounts that exceed a 1% threshold and are greater than $10 based on a cumulative total of contribution reports as well as individual payroll report and adjustment entries, require resolution as part of completing the contribution posting process. The total of employee deposits for the period entered is used to calculate an expected employer contribution amount, which is compared to the sum of the amounts entered by the employer on the Employer Portal. Underpayments and overpayments for the period that exceed the 1% threshold are communicated to the employer, and underpayments are tracked by Employer Plan Management until resolved.

Reporting Process

Authorized employer contacts are required to enter total employee and employer contribution amounts when uploading their payroll or adjustment report file through the secure TCDRS website. TCDRS portal users with Security Administrator and Payroll Administrator roles are authorized to report payroll and adjustments. The Compass system sums the total contribution amounts for the employer representative prior to completing the upload process. The payroll upload automatically creates an accounts receivable transaction for the employer in the Dynamics GP accounting system. The receivable is posted in Dynamics GP by an automated process. The upload also separately triggers a payroll case in the Compass workflow management system used to control the reporting process. Payroll contribution files are stored and processed from the Compass case directly. The Compass workflow case tracks payroll reports available for processing.

Detailed employee deposits and payroll reporting invoices are maintained in segregated systems. A separation of functions also exists between the two processes and applications. The payroll process creates a unique employer receivable for the total contribution amount in the Dynamics GP application separate from the member deposits uploaded through a Compass case. The Finance team accesses and manages the total contribution amount and employer funds received through Dynamics GP and the Employer Plan Management team completes the employee deposit upload and verification process in Compass. Ultimately, the separate processes are reconciled weekly as part of an ESF Balancing review by the Finance team and verified monthly by EPM to help ensure accurate funds and employee deposits have been posted. Additionally, on a weekly basis the Finance team reviews the “Unapplied Documents” report identifying unapplied debits and credits in the Dynamics GP Receivable module. The report is

provided to the Employer Plan Management team monthly, at a minimum, so that identified reconciling items can be timely researched and resolved.

Additional Employer Contributions

Controlled procedures also exist for processing additional employer contributions. An employer Decision Maker, Payroll Administrator or Security Administrator is required to authorize an additional employer contribution as a plan election. Authorized employer representatives (Decision Maker or Security Administrator roles) can then enter an additional employer contribution amount through the secure TCDRS website, which triggers an accounts receivable transaction in Dynamics GP and an additional contribution workflow case in Compass. Once the additional contribution payment is received, an offset to the Dynamics GP receivable balance will be posted. The Employer Services team manages the authorization and processes the Compass case, and the Finance team posts the funds received. The separate authorization, processing, and funds posting are reconciled with any outstanding issues resolved. A year-to-date schedule of lump sum contributions received, along with a detailed listing of unfunded lump sum contribution receivables, is prepared monthly by the Finance team and distributed to the Employer Services and Actuarial Services groups for review and comment.

Report and Payment Tracking, Posting, and Reconciliation

Employer accounts receivable amounts are tracked separately by the Finance and Employer Plan Management teams through Compass and Dynamics GP. Compass workflow cases also identify outstanding reports available for processing. Employers with mismatched deposit reports and payment contributions are reviewed by EPM and resolved daily.

The sum of detailed employee contributions is compared to the reported total employee contribution amount to help ensure correct deposit amounts are processed in the pension system. Compass automatically performs validation functions during the employee contribution upload process to help ensure deposits exactly match the total amount submitted by the employer via the Employer Portal. If errors are identified during the employee contribution upload, a segregated process is utilized to void the accounts receivable invoice in Dynamics GP with a corresponding cancellation of the payroll case in Compass. The employer's Security Administrator or Payroll Administrator subsequently submits a corrected payroll contribution file for processing. Deposits cannot be posted to member accounts unless they reconcile to the totals submitted by the employer via the Employer Portal that have been integrated into both the Compass case and the Dynamics GP systems.

If a member's Social Security Number (SSN) and associated financial account do not exist for a reported employee contribution, Compass will reject the entire payroll report. The employee account information is resolved by an authorized employer representative (Security Administrator, Benefits Administrator or Payroll Administrator portal role) upon notification by the Employer Plan Management team. This process assures contributions are properly associated to the correct employee. Compass denies processing files until SSN validation errors are corrected. Contributions received for closed accounts are treated as exception cases if validations fail in-service distribution rules that evaluate timing and number of deposits with employment termination dates. Exception cases are resolved by Employer Plan Management. The first and second contributions received for an account closed less than a month are considered standard and are processed automatically.

All employer payments processed correspond to a Dynamics GP accounts receivable transaction created from the employer's website entry or the certified document received. The Finance team reviews outstanding accounts receivable balances at least weekly to help ensure invoices are correct and payments are accurately applied to the employer reported amounts. Any differences in paid amounts and accounts receivable balances, including unapplied payments, are researched and resolved. Funds received are also reconciled daily and monthly as part of the TCDRS bank reconciliation process. A bank cash report is balanced with Dynamics GP daily to help ensure all monies received were correctly recorded. On a monthly basis, or more frequently as necessary, an Unapplied Receivables report is

prepared by Finance and sent to Employer Plan Management that reflects outstanding receivables or unprocessed credits that are researched, confirmed with review of Compass cases to confirm the over or underpayment and communicated to the employer.

TCDRS members can verify deposit activity and account information through the TCDRS website or their Annual Statement. Employers can confirm all monthly account and payment activity through Employer Activity Statements that are posted to the website monthly. Both reports provide an opportunity to review and confirm posted transactions.

ACH Debit Process

A controlled ACH debit approval process is applied between separate teams using payment verification reports and Dynamics GP receivable balances. The Finance team confirms ACH debit amounts correctly correspond to Dynamics GP accounts receivable balances and all adjustments are included for the reporting period. Employer Plan Management separately compares payment amounts using an ACH debit tracking tool. Reconciled amounts are approved by both teams and included in the ACH debit file while any receivable differences are resolved prior to processing. Total record counts and debit amounts included in the approved ACH report are confirmed with ACH debit bank file totals to help ensure all finalized amounts were imported and generated correctly for bank processing. A segregation of duties between Finance team members is also applied to help ensure control of the file transmittal process. An individual with isolated access rights creates and loads the ACH debit file while a different individual releases the file to the bank.

Income Allocations

Control Objective 3: Controls provide reasonable assurance that income allocations are completely and accurately posted to employer and employee accounts based on amounts approved by the Board of Trustees.

Funds receive an income allocation based on statutory requirements and net investment results. Investment income calculations pertaining to each fund are reviewed by the Finance team and then separately confirmed by the Actuarial Services team before and after income is allocated.

Tracking and Auditing Investment Earnings and Income Allocation

The Investments team collects and reports investment return information on a daily basis to track income throughout the year and distributes to the TCDRS executive team. Investment results and the annual income allocation are reviewed and audited by an external auditing firm as part of TCDRS's financial report audit. Income allocation is also published through supplemental schedules in the TCDRS Annual Comprehensive Financial Report that is posted to the TCDRS website.

ESF Interest Allocation

Changes in the ESF are reconciled between Dynamics GP and tEDS on a monthly basis by Finance for transactions not related to monthly contribution reporting, which is controlled through automated processes in both GP and tEDS. In addition, each month, Employer Plan Management reconciles funds received and recorded in GP for member service credit purchases to tEDS entries for those deposits in member accounts. These confirmed individual ESF beginning-of-year balances are used to calculate member account interest.

Interest based on the member's beginning-of-year balance posts to member accounts on a monthly basis. Interest transactions are systematically applied to member accounts through a scheduled system procedure. The job circulates confirmation of successful completion or will trigger an exception notification if issues arise. For benefits with an effective date prior to an interest transaction effective date (typical for death withdrawals and survivor benefits and occurring on a less frequent basis for service and disability retirements), interest transactions are automatically backed out of the account as part of the benefit inception processing through Compass. These automated interest transactions are reviewed for exceptions on an annual basis.

Summarized interest transactions for each employer are integrated into Dynamics GP and posted by the Finance team monthly. The Finance team reconciles these amounts to the Compass SSRS ESF Interest report prior to posting.

SAF Income Allocation

Income allocation for each employer is based on reconciled beginning of year account balances and an allocation rate approved by the Board of Trustees in accordance with TCDRS policy and resolutions. The positive or negative allocation to each employer's SAF account is equal to the total allocation to the plan less the statutory allocations related to each employer. Board of Trustees' minutes are stored in FileNet for confirmation, control and records retention.

The SAF allocation is calculated using verified allocation formulas as defined by the board and a Dynamics GP trial balance report. The amounts are confirmed through a quality assurance process completed by the Actuarial Services team before posting to the Dynamics GP general ledger using an integration tool that helps ensure data integrity. Total allocation is verified prior to posting the general ledger entries using system generated balancing reports. The Finance team finalizes the process by reconciling total income allocation amounts to employer SAF balances and recalculating the allocation for a select sample size.

General Reserves Income Allocation

The Finance team also calculates available income (or loss) to allocate to the Endowment Fund. Available income is determined after statutory allocations are verified and Board of Trustees approved SAF income allocations are confirmed. The Finance team also uses the Dynamics GP trial balance report and an investment income calculation tool as the basis for determining the allocation amount and the appropriate journal entry is made and confirmed in Dynamics GP. All documentation is retained for reference and confirmation.

Fund Balances

Control Objective 4: Controls provide reasonable assurance that fund balances are reconciled and reported accurately and completely.

The ESF contains an account for each member. Compass acts as a subsidiary ledger for member-level activity. A summary of ESF transactions by employer is maintained in the Dynamics GP general ledger.

The SAF contains an account for each participating employer to fund retirement benefits solely for that employer. Dynamics GP is the system of record for the SAF, with the pension system recording detailed activity related to retirement transfers and monthly retirement benefit payments that are subsequently recorded at the employer level in Dynamics GP. All employer balances are reviewed monthly for reasonableness with exceptions managed using Dynamics GP general ledger information.

Employer level and system-wide asset information used by the consulting actuary is reconciled by the Finance team and reviewed by the Actuarial Services team. After the verification of annual activity and year end fund balances are completed, this information is sent to the consulting actuaries for purposes of conducting the annual valuation process.

Beginning and end-of-year balances and changes in the ESF and SAF are submitted by the Finance team to the consulting actuary as part of the accounting valuation data. These reports are reconciled, documented and verified by the Finance team. Fund activity and balances, including the information in these reports, are audited by an external auditing firm as part of TCDRS's Annual Comprehensive Financial Report process.

Changes in ESF and SAF

Each addition and deduction component of the "Changes in ESF" and "Changes in SAF" are reviewed monthly in addition to a final annual reconciliation prior to forwarding to the consulting actuary.

- An automated process is used to generate GP entries and Compass case control data from employer web entries. Employee payroll deposits to tEDS cannot be posted unless the deposit total matches the control data. These entries are confirmed by comparing the funds received for these transactions to data in GP and tEDS and resolving any differences. Total employee deposits and related employer contributions can be further confirmed by employers through a monthly Employer Account Statement that reports financial transactions posted to each employer's account.
- Interest is credited to member accounts monthly based on the member's beginning-of-year ESF balance and posted to Dynamics GP on an employer-level basis. The Finance team completes a final reconciliation of ESF interest each year by comparing Compass total interest transactions to the Dynamics GP general ledger.
- Allocated Net Investment Income to the SAF is approved by the Board of Trustees annually. Calculated allocation amounts are completed by the Finance team and confirmed through a quality assurance process completed by the Actuarial Services team. Confirmed income allocation amounts are integrated into the Dynamics GP general ledger to help ensure data integrity. Total amounts are verified prior and subsequent to posting entries to the general ledger using system generated balancing reports.

All other ESF and SAF entries (retirement transfers, withdrawals, monthly retirement benefit payments and Endowment Fund transfers) are systematically integrated between Compass and Dynamics GP through a monthly batch process. A monthly GP vs tEDS analysis and a fund balance reconciliation process are performed to confirm the integration using SSRS reports for each transaction type.

Endowment and Expense Fund

The Finance team calculates a positive or negative amount to allocate to the Endowment Fund. This amount is determined after statutory allocations are processed and verified, and board-of-trustees-approved SAF income allocation is confirmed. The Finance team uses the Dynamics GP trial balance report and an investment income calculation tool as the basis for determining the allocation amount.

For GASB 67 Fiduciary Net Position purposes only, once the allocation is finalized, the Finance team allocates the Endowment and Expense fund balances to each employer based on their end-of-year ESF and SAF fund balances. The Actuarial Services team confirms the allocation. The allocation of Endowment and Expense fund balances to participating employers is reviewed by the independent consulting actuary. Amounts prior and subsequent to the disaggregation are verified for accuracy using a fund workbook maintained by the Finance team and Dynamics GP trial balance reports.

Fiduciary Net Position Schedule

Disaggregated fund amounts by employer are reconciled by the Finance team. Each employer's net position components are reconciled as part of monthly contribution and benefit processing and annual income allocation balancing. The ESF and SAF are all balanced on a monthly basis and prior to being applied as the basis for determining disaggregated allocation amounts.

A verification of calculations is performed by the Finance team and separately verified by the Actuarial Services team. Individual employer amounts and cumulative amounts are re-calculated during the verification process. The same calculations are completed by the consulting actuary for verification if there has been a change in methodology. The calculations are additionally audited by an external auditing firm as part of the Annual Comprehensive Financial Report.

Distributions

Control Objective 5: Controls provide reasonable assurance that distributions (i.e., disability, partial lump sum, withdrawals, and service retirements) are authorized and processed accurately and completely.

Distribution processing is controlled through documentation requirements, separation of duties, written procedures, SSRS reporting and validation (using tEDs data), Compass case tracking, quality assurance steps and internal audit reviews. The following are various types of distributions available to former employees or beneficiaries depending on benefit eligibility, employment status and benefit plan provisions:

- Service and disability retirements
- Partial lump sum payments at retirement
- Death benefits
- Withdrawal of contributions

Distributions can be a monthly annuity or a one-time payment. The basis of all distributions is the employee account balance, contribution payroll reporting, and income allocation control objectives and procedures. Benefit calculations apply plan provisions as an additional calculation element supported through benefit-plan-related control objectives. Additionally, retirements, deaths, withdrawals and member account reports are posted to the Employer Portal on the TCDRS website for employer review.

To help ensure separation of duties, contribution and distribution processes are separate business departments with their own unique system access. Employer Services manages employer benefit plan information; Employer Plan Management processes member setups and contributions; the Finance team processes employer receivables and contribution payments; and the Member Benefits team processes distributions. System access among functions is reviewed every six months through an internal TCDRS access recertification process to help ensure duties are separate. An Account Balance Exception report is reviewed by both Employer Plan Management and Member Benefits staff to identify and review any closed member accounts with a positive balance, or any account with a negative balance, caused either by contribution reporting or payment processing that would create an error in the benefit that is calculated and paid.

All distributions are initiated by submitting forms or applying through the secure TCDRS website or alternatively through the call center. Required employment termination dates from the employer is provided via the Employer Portal. Additional supporting documentation, including proof of birth or a death certificate, and a proof of identity may be required based on the type of distribution and authentication results. Documents received via mail or through a secure upload process are saved into FileNet, TCDRS's document repository system. The scanned or uploaded documents create a Compass case or associates it with an existing case to track processing and create an audit trail in addition to retaining distribution paperwork. The data entered online through the web application or via a representative through the phone application is used to create a Compass case used for tracking processing and generating benefit payments and also creates a document of all data submitted by the applicant.

If information is missing or the benefit application is incomplete, an additional documentation request is forwarded to the applicant. The request for outstanding information is tracked and monitored in the Compass workflow case. Member Services reviews payment accuracy by reviewing queries for accounts with negative and positive balances at least once per month.

ThreatMetrix, inclusive of Emailage and PhoneFinder, is a third-party tool that is used to assist TCDRS with the identification of a participant applying for a retirement, a withdrawal, or a payment address update. For Emailage, a user can receive either a "low" result or a "high" result. For PhoneFinder, a user can receive either a "pass" result or a "fail" result. For ThreatMetrix, a user can receive either a "pass"

result or a “reject” result. These results are based off several scenarios such as an email or phone number not matching the registered participant, the primary phone area code is not in the same state as the primary address, the account address and the participant’s true geographic location mismatch, or the input, true, proxy IP is outside the US CA GB. For applications coming online, ThreatMetrix considers factors such as network connections, IP addresses and other forensic data gathered during a user session. Emailage and PhoneFinder are used when applications are coming via the phone or online. The user’s email address is given a risk result based on such things as the historical use of that email address. PhoneFinder verifies the applicant using their phone information and confirms the phone used for Multi-Factor Authentication belongs to the member. If PhoneFinder fails, Emailage is high, or ThreatMetrix provides a reject result the participant will fail the Authentication case in Compass, and a Security case will be created for an Anti-Fraud Analyst to review. If PhoneFinder or Emailage pass (i.e., have a low result) and ThreatMetrix provides a pass result, the participant is able to proceed applying for a retirement, a withdrawal, or a payment address update. The Security case triggers an email with a link for the member to upload an ID; once the ID is received, the Anti-Fraud analyst reviews the documentation provided. In determining whether to approve the Security case, the analyst considers factors such as the member's demographic information history, any prior account or call center activity and demographic search results used to assess the member’s identity. Once the member's identity is verified, the analyst approves the Security case which allows for the associated payment case to be processed. If it is determined that it is not the member who submitted the application, Anti-Fraud can reject the Security Case, which will close the associated withdrawal, retirement or payment address case. By The Director of Anti-Fraud reviews escalated cases as well as spot checks analyst work for quality assurance purposes.

ThreatMetrix access is managed by Infrastructure Security team that is separate from the Website team that manages configurations. Policy access is restricted to a limited number of individuals, including the Director of Anti-Fraud, the LexusNexis ThreatMetrix Analyst assigned to TCDRS’s account. Changes to policy or technical configurations are subject to TCDRS’s change management process, specifically a management review and approval before changes are made. This also includes a post-implementation review of the ThreatMetrix change. Emailage and PhoneFinder are not configurable by any personnel at TCDRS.

TCDRS uses a third-party tool, Plaid, to validate banking information used to make retirement and withdrawal payments. Plaid retrieves bank account and routing numbers for direct deposit payments to members and retirees by directly connecting to their account using specific bank credentials entered and owned by the member. The Member Portal on the TCDRS secure website uses an authenticated API to initiate the integration and securely transmit encrypted data from Plaid to TCDRS. Access to configure Plaid is restricted to the approved website architect team and temporary access is granted to developers as needed to manage production support issues or complete development work.

Service and Disability Retirement Distributions

Service retirement applications can be completed through the secure TCDRS website or the call center. Call center applications trigger a DocuSign with the member’s electronic signature required for formal approval prior to processing. Online benefit applications are completed by the member with a receipt summary available for reference. Both channels include an authentication step to ensure benefits are paid to the intended member. Additionally, an annual review is conducted on death cases for which a user with the ability to conduct the quality assurance review performed a review of their own case. Any such cases identified are investigated and resolved. Business exceptions that require Member Benefits review are included in each channel to ensure accuracy of the application and mitigation of risk. As of January 2024, survivor benefit applications for deceased member benefits follow a similar process with a quality assurance check for beneficiary verification documentation requirements.

Procedures and verification steps help ensure retirement eligibility is calculated correctly:

- Service credit entered into Compass separate from the monthly payroll reporting process requires documentation and entry verification by a different team from Member Benefits.
- Member birthdates are managed by employers and used to determine benefit eligibility. Beneficiary proof of birth is systematically verified by a Compass integration to LexisNexis. If the age cannot be verified, proof of birth documentation will be requested.
- Disability applications require independent medical board approval.

The Benefits team conducts a review of annuity and partial lump-sum calculations as an internal monitoring step annually and as part of testing major system builds.

ESF receives employee account balance transfers to the SAF when an employee retires for the purpose of funding the employee's retirement benefits. The monthly annuity payment is disbursed from the SAF. Service and disability retirement transfers from the ESF to the SAF are systematically integrated through a monthly batch process between tEDS and Dynamics GP. The Finance department reconciles retirement transfers from ESF to SAF and ongoing annuity payment amount activity in tEDS and Dynamics GP on a monthly basis using the "3XXXX" fund balancing analysis.

Partial Lump-Sum Payments at Retirement

If an employer authorizes partial lump-sum payments at retirement, former employees applying for a monthly retirement payment can also request a single payment up to their accumulated account balance. The benefit plan provision is controlled through the annual employer plan decision-making process.

Members eligible for partial lump sum payments at retirement enter the elected amount and distribution type online or through the call center when applying for retirement. The call center channel requires members to electronically sign an application summary prior to processing the benefit. Systematic Compass business validations add controls and confidence to the partial lump-sum payment process:

- System validation prevents the entry of partial lump-sum payments unless authorized as a benefit plan provision by the employer.
- System validation prevents a partial lump-sum payment amount from exceeding the amount available in the former employee's account balance.
- System validation automatically reduces the monthly benefit calculation by the partial lump-sum payment processed.
- System validation requires an electronic signature to process the partial lump sum payments.

Survivor Benefits

A designated beneficiary may collect a survivor benefit if an employee or retiree dies. Survivor benefit options are based on the member's benefit eligibility or the retiree's benefit option selected.

For applications submitted prior to January 19, 2024, beneficiaries of deceased members and annuitant survivor benefit calculations and account set-up required specific documentation and included a quality assurance step from a separate team member to ensure data is correctly captured. Documentation and review requirements included a death certificate of the member and a proof of birth and identity from the beneficiary. As of January 19, 2024 and beyond, deceased member survivor benefit calculations are systematically calculated and do not require quality assurance. Certain types of beneficiaries are systematically verified with required documentation managed by Compass and reviewed by the Benefits team (and possibly Legal team). If formal beneficiary documentation is required, then a quality assurance step is included before creating the beneficiary's account. Compass systematically verifies the member's date of death and the beneficiaries date of birth using LexisNexis. Compass business rules and validation

apply confidence in processing deceased member survivor benefits. Compass validation and exception procedures add additional control and confidence to annuitant survivor benefit processing:

- System validations in Compass automatically expire annuity payments for certain benefit options when a retiree dies.
- System validations in Compass only allow a beneficiary account to be created for certain retirement options and associated survivor benefit expiration dates.

In addition to these pension system controls, a manual review of data included in the monthly payment file validates the annuity payroll was complete and accurate. Member Benefits and Finance reviews data from Compass cases, tEDS and the payment files in a monthly reconciliation process. Exceptions are reviewed and resolved prior to finalizing benefit payments. Lump sum survivor benefit reserve payouts are included in the actuarial valuation process to ensure funding remains stable.

A weekly comparison of active benefit recipient data to historical death records and obituaries maintained by PBI Research Services and a monthly comparison of active benefit recipient data to records maintained by the Texas Department Vital Statistics is performed to identify any payments that need to cease due to retiree deaths. Payment status is confirmed or managed as part of this verification process.

Withdrawal of Contributions and Interest

Former employees can elect to withdraw their accumulated contributions and interest as a single distribution payment. Withdrawal applications can be submitted by paper, phone or online. Online and call center channel applications use an authentication process as a verification of identity. Call center channel applications require an electronic signature from the member to confirm the withdrawal details. An electronic signature is required prior to processing the payment. Online applications are entered directly by the member with a receipt and communications provided for confirmation. If application data is entered by the call center, the member will verify the information (quality check) and provide their signature to complete the application. For all applications, employers must provide an employment termination date via the Employer Portal that is earlier than the distribution date. This requirement is validated within Compass and no benefits can be paid prior to the employment termination date. All documentation is stored in FileNet, including a receipt of the online benefit application, and a Compass case is created for tracking and verification.

Compass validation and exception procedures provide additional control and confidence to withdrawal processing:

- System validation in Compass only allows distribution of the benefit after the employee’s termination date has passed.
- System validation only allows payments to be processed for the available account balance. A payment reconciliation case provides assurance that the payment exceptions are reviewed before being issued.
- System validation automatically processes benefits for online applications that, at the time of application, have an employer entered termination date, have passed the Authentication Case, and are below $100,000. Member Benefits acknowledges withdrawals equal to or greater than $100,000 and Anti-Fraud reviews any Security Case created due to a failed Authentication Case.
- An SSRS report, Weekly Recon Exceptions, is reviewed to identify pending payments that do not reconcile to the refund payable.

Monthly fund balancing procedures are performed by the Finance team in the “3XXXX” fund balancing analysis, a process which helps ensure that year-to-date withdrawal activity per Dynamics GP agrees with Compass pension system transaction activity as depicted on the corresponding withdrawal transfer

report. Additionally, the Finance team prepares a comprehensive monthly ESF balancing schedule reconciling Dynamics GP activity to the Compass pension system activity.

Annuity Payment Adjustments

Monthly annuity payments can be increased for cost-of-living adjustments if authorized by the employer as part of the annual benefit plan decision. The employer-authorized cost-of-living adjustment can be based on a percentage of the change in the Consumer Price Index (CPI) or a specified percentage increase, not to exceed the maximum cap set by the Board of Trustees. Employer cost-of-living annuity adjustment authorizations require a quality assurance step that is completed by the Employer Services team.

Upon the request of Actuarial Services, the Information Technology team loads the annual CPI into a database table in tEDs used to calculate annuity adjustments. IT confirms the data was successfully loaded. The Actuarial Services team then verifies that the CPI figure has been posted successfully.

After Employer Services verifies that all plan changes have been updated in Compass, the IT team applies COLAs to annuity accounts. Verification is completed by Benefits using ad hoc confirmation queries run by IT.

The Member Benefits team completes a thorough verification of cost-of-living adjusted annuity amounts prior to issuing benefit payments. A sample of adjusted annuity amounts is manually calculated and verified with the provided queries. These calculated annuity adjustments are compared to the increased annuity amounts captured in Compass.

The Member Benefits team also reviews a SSRS annuity change report that identifies annuity payment adjustments exceeding a threshold on a monthly basis. These reported annuities are researched and confirmed or corrected. Any changes are documented for reference and control.

Payment Generation

Controls and policies have been implemented to reduce payment generation risks. A daily positive pay process involves sending a file listing checks printed and voided by TCDRS to the bank to help ensure that payments processed reconcile to positive pay data and voided payments are denied. In addition, the Member Benefits team reviews a positive pay exceptions report and resolves any issues as part of the daily process. A daily file is received from the bank to update cleared checks in Compass.

All outstanding annuity checks are automatically voided 90 days after issuance. Annuity check payments presented to the bank for payment or paid by the bank are reviewed through a bank account reconciliation process in Finance to confirm any voided payments that have been paid match positive pay exceptions approved by Member Benefits. All exceptions require confirmation and a timely documented resolution. In addition, the Finance team performs monthly bank reconciliations comparing TCDRS payments, void, and outstanding check amounts with the corresponding bank balances. Reconciling items are researched and resolved in a timely manner.

Information Technology Controls

Applications Maintenance

Control Objective 6: Controls provide reasonable assurance that modifications to applications are authorized, tested, approved, documented, and implemented.

Maintenance and development of additional application functionality is accomplished through an organizational methodology that applies application analysis, a three-environment migration process, source control, documentation through Azure DevOps, and a formal sign-off and managed implementation. Depending on the project effort, the migration path will follow hot fix for production support fixes and enhancements and a Project migration path for enterprise-project, longer delivery efforts. Both paths start in a development environment and are tested in the hot fix or project environment.

Application modifications can be deployed as part of a project development effort, system functionality enhancements, application upgrades or patches, defect production support issues, architecture changes, or service or process expansion initiatives. Modifications can range from an isolated application to system enterprise level impact. All application development must follow a controlled process that includes impact analysis, design, development, testing, approval and implementation. Due to the TCDRS enterprise architecture, overarching system impact is also assessed.

Change Management and Issues Tracking

Change management governance policies and procedures have been implemented to analyze change requests, including emergency changes. Business and technical requests are documented in Azure DevOps for review, prioritization and impact assessment. An IT and business director level prioritization group reviews application change requests regularly. The group reviews planned changes to help ensure that projects, initiatives, enhancements and general modifications are prioritized, tested, approved and implemented. Development initiatives are balanced with the goal of maintaining reliable availability of the enterprise production environment that supports customer service and business processing.

All application defects and errors are managed through the Enterprise and Help Desk with issues, changes, documentation, testing, approval and deployment captured in Azure DevOps.

Development Process and Control

TCDRS application development strategy includes a documented and controlled promotion path using distinct development, testing and production environments that follow a hotfix or project release path. All environments are fully maintained to help ensure all application changes are developed, tested and approved using independent servers, databases and application interfaces from the production environment. Production improvements and bug fixes follow a development-hot fix-production path. Project work follows a development-project-production path. Testing occurs in the hot fix or project environment and the release process to production includes a build to the test environments to help ensure all code base remains aligned.

All application changes follow a controlled deployment process throughout each environment. All code changes are checked into Azure DevOps source control or compiled into a repository or package for control, documentation and managed promotion.

The organized strategy is consistently applied to all application development efforts:

- Approval for work is necessary by IT and business management to help ensure that development efforts are aligned with organizational priorities and initiatives.

- Application issues and project releases are logged and documented using Azure DevOps. Work is assigned based on available resources and development approach.
- Development and coding are conducted in a development system environment. Unit testing is completed as part of development and quality assurance (QA) with identified issues resolved before promoting changes.

Integration or hot fix is the next environment in the deployment process for production support issues, production code fixes, and production-specific enhancements. There, IT and business confirm the impact that application changes have on the enterprise architecture and ensures data integrity among all systems. Upon successful test results, database administrators apply database object changes and application and database owners apply code changes to the integration/hot fix environment. Any necessary changes are made in the development environment and re-deployed to the appropriate testing environment for final review and approval.

User Acceptance Testing or project is the testing environment used for enterprise project work that requires a longer lead time and has additional enterprise-level impact. This is also where business users confirm all changes and complete regression testing, as needed, of impacted applications. Upon successful test results application and database owners deploy code and database changes between development and UAT environments. Any necessary changes are made in development and promoted through the environments.

Production deployment of application changes requires documented management approval with successful test results. Depending on the release scope, business users and/or IT application owners complete basic testing following implementation to ensure deployment was successful.

Segregation of duties between developers, IT testers, business testers, database administrators and management is maintained throughout the development, code release and testing process for all application environments including Dynamics GP, Compass, and the TCDRS website, as well as SSRS reports.

Application changes are tested and approved in integration/hot fix or user acceptance/project environments by non-developer team members within IT and business departments. Test cases are approved by technical and business teams based on the features developed. IT quality assurance performs technical and unit testing. Business testers complete additional end-to-end and regression testing of all impacted applications at the enterprise level using documented test scripts to help ensure all application functionality is accurate and complete.

Build Process

Application deployment requires IT and business director or designated manager approval prior to releasing to the production environment. Depending on the release scope, application deployments involve collaborative IT and business resources, Infrastructure Services team, designated testers, developers, database administrators, system architects, management, and business representatives.

Infrastructure Services will provide access to application environments with documented approvals or access is granted through privileged access management workflow process. Application Administrators deploy code changes to production applications. If production deployment is performed by a developer due to the type of application changes, temporary and specific access is documented, exclusively assigned and monitored. Temporary access to developers to complete deployments is granted through a privileged access management workflow that initiates a password checkout process. If necessary, Infrastructure Services will also provide access to application environments with documented approvals. Access is routinely reviewed to ensure that access was appropriately managed with approved deployments. Developer and database access reviews are completed through an internal review process that occurs on a quarterly basis. A combination of management approval, pre-deployment testing, source control and build oversight provides confidence in the deployment process.

A build plan is documented and reviewed by all IT team members for enterprise project deployments prior to promoting application changes to production. The plan details the start and end times for each build task including initiating system stop scripts, completing database backups, promoting code changes, making configuration changes, running any special scripts and completing any additional tasks necessary for successful implementation. Each build plan contains a back-out strategy in the event complexities arise during deployment.

Logical Access

Control Objective 7: Controls provide reasonable assurance that logical access to programs and data is granted to authorized individuals.

Access and Passwords

Requests for new access, changes to existing access or removal of rights for applications, database, operating system and network are documented. Access for new users are authorized and requested by Human Resources and the hiring manager or department director and submitted to the Help Desk for implementation. Changes to access for existing users are authorized and requested by the user's supervisor and submitted to the Help Desk. Upon termination, an employee or consultant account is immediately disabled. Access management is documented through the SysAid Help Desk system.

TCDRS has a password policy outlined in its Information Technology Security Policy. Access to all TCDRS information resources are protected through usernames and passwords. The TCDRS password policy for employees includes:

- Employees may not share their passwords.
- Employees may not post written lists of passwords in their work area or on laptops.
- Passwords used internally may not be used for external sites.

The Infrastructure Services team enforces the following password policies using a Windows domain security policy:

- Passwords must be changed every 60 days.
- Passwords must not have been used in the previous five passwords.
- The password must not contain all or part of the network user name.
- The password must be at least six characters in length.
- The password must contain characters from three of the following four categories:
  - English upper-case letters
  - English lower-case letters
  - Base 10 digits
  - Non-alphanumeric characters

Exemptions to the above policy are allowed in limited circumstances (e.g., not enforcing account expiration for specific system or service accounts.) These exemptions are noted in the policy and approved by management. Infrastructure Services produces a monthly report of all Active Directory user accounts that have not been utilized in 90 days or more. Identified dormant accounts are referred to appropriate department directors for removal approval. Accounts for non-TCDRS employees are referred to the Director of Infrastructure and Security or designated manager. Accounts are removed when requested by the Infrastructure Services team.

Remote access is controlled through usernames and passwords that conform to the TCDRS password policy. Additionally, multi-factor authentication (MFA) is enabled for all remote access and remote access protocols are encrypted for further control.

A consultant and remote user password policy is applied to help ensure access is restricted to authorized individuals based on job requirements. Consultant credentials are limited to remote access to

development environments. A consultant's network access automatically expires after 90 days and is reviewed monthly by the hiring manager.

Application Access

Access to TCDRS's business applications is granted by security administrators through written SysAid Help Desk requests. The passwords are set to expire in compliance with the IT Security Policy. Users are locked out after a determined number of invalid attempts and applications are configured to time out after a specified period of inactivity.

Access to certain functionality and processing capabilities is controlled through system-defined user roles. Separation of job functions is also supported through limited system access. For example, Employer Plan Management retains access to upload payroll contribution reports but cannot access system functionality to process distributions. Similarly, the Finance team can access Dynamics GP to process and balance employer funds but cannot access Compass member contribution functionality. Workflow management is also controlled through system access. Certain user profiles are established to enable or limit tasks that can be performed. For example, elevated user access groups can complete a quality assurance step that would be inaccessible to different profiles.

Employers are required to login to the TCDRS Employer Portal website using secure credentials that are associated with certain access and functionality roles. The established roles limit access to perform certain web functions. Password requirements follow security guidelines to help ensure access is protected. Additionally, failed website login attempts will automatically disable access. All website passwords are encrypted when stored in Okta.

Permissions

The practice of "least privilege" is applied when granting permissions. Permissions are granted based on job requirements. Users are not granted administrative rights to their desktop or laptops unless approved by the Director of Information Technology or the Director of Information Technology's designee.

Permissions to network directories and system applications are routinely audited by the Director of Internal Audit department through a recertification of security rights process. The frequency of audit review is based on the risk level of the application prescribed in the Information Access Recertification Policy. All core processing systems have an access review completed every six months while lower risk applications are reviewed annually. The Director of Internal Audit department reviews access to the Compass application every six months to help ensure access is necessary and appropriate for job responsibilities. Dynamics GP application access is reviewed annually as part of TCDRS's recertification policy. Administrative access to third-party service providers JPMorgan, ThreatMetrix, Plaid, and Okta is reviewed every six months, as is internal access to the Employer and Member Portals.

The Director of Infrastructure and Security or other designated manager reviews SQL server database access accounts quarterly to confirm that production access is appropriate and secure. Database access levels are reviewed for the Dynamics GP database and the enterprise SQL database to help ensure access is limited and necessary.

The Director of Infrastructure and Security or other designated manager review Active Directory accounts, including domain administrators and other privileged users on a monthly basis. The review is documented, along with any necessary access modifications, by the security administrator upon completion. The Director of Infrastructure and Security performs final confirmation of permissions.

Administrator access to production environments is restricted accordingly:

- Database Administrators only retain administrator access to production databases through the privileged access management system

- The Infrastructure Services team retains administrative access to production application and database servers.
- Application Developers' administrative access is limited to development environments with read-only access to production databases. Temporary access to application production servers is granted to deploy specifically approved, documented code releases with access rights removed upon completion and verification.
- If Developer's access to production systems is required for problem resolution or production assistance, management is informed of the need for the access and, where possible, activity of the developer is tracked, monitored and reported to management.

TCDRS also maintains laptop, wireless, handheld and email security policies to protect from unauthorized access and use, and possible corruption of systems.

Firewalls

Firewalls are used to limit ports available to external users and to limit access to internal computing resources: disaster recovery firewall, website firewall and an external Internet firewall. TCDRS protects all local area networks (LAN) from unauthorized access by the use of firewall devices. TCDRS uses Forcepoint Next Generation Firewall (NGFW) for network firewalls. The Forcepoint NGFW features an Intrusion Protection Server (IPS) that detects attempts to gain unauthorized access and alerts Infrastructure Services security staff for review and confirmation.

As a best practice, the Infrastructure Security Administrator conducts a quarterly comprehensive review of firewall rules.

TCDRS applies firewall devices to regulate access protocols and guard against attempts to gain unauthorized access to local TCDRS networks. Vulnerability assessments are conducted annually to test internal and offsite network environments. Additionally, a website code review and a penetration test are conducted periodically by a third-party security assessment firm to help ensure all security objectives are met and risks are defined and mitigated. Vulnerabilities are evaluated and corrective actions are implemented pursuant to the security level required to maintain business continuity.

Data Transmission

Website employer payroll reports, new member enrollment information and employee termination dates are submitted through unique login credentials using a secure connection.

Backups

Control Objective 8: Controls provide reasonable assurance that data and systems are backed up on a scheduled basis, stored in an offsite location and available for restoration.

All servers are backed up on a daily backup schedule. Differential SQL data backups are completed nightly and full SQL data backups are completed weekly, with nightly replication to offsite storage of transaction logs.

Backup, Recovery, Restore

Backup recovery processes have been established for all mission critical systems. Production servers are backed up offsite daily and transaction logs are backed up every 30 minutes between local production servers and nightly to an offsite backup appliance. Application and database production server backups are also conducted daily and immediately replicated offsite at the completion of the backup. Recovery assurance logs are monitored to help ensure that the backups replicated offsite are available to be restored.

Offsite backup facility retains backup history for no more than 30 days, with a maximum retention period set for each server. These backups are automatically purged when the retention period is reached.

Backup Tracking and Management

Email communications are forwarded to database administrators and the Infrastructure Services team to confirm backup completion or define errors. Monitoring tools are implemented to notify database administrators when backup attempts fail. Backup failures are investigated and resolved in a timely manner using logs, messaging tools and exception reporting. Access to backup schedules is limited to database administrators and certain Infrastructure Services staff based.

Other Information about Management's Description

TCDRS's control objectives and related controls are included in Section IV of this report, "Texas County & District Retirement System's Control Objectives, Related Controls, and KPMG LLP's Test of Controls and Results." Although the control objectives and related controls are presented in Section IV, they are, nevertheless, an integral part of TCDRS's description of controls.

Complementary User Entity Controls

Many aspects of the pension processes at TCDRS are dependent on the processes that occur at the county or district employer (also known as a “user entity”).

The items listed below are internal control responsibilities that TCDRS believes should be present at each participating county or district. Each county or district must evaluate its own internal controls to determine if the following are in place and operating effectively. The following list is intended to address only those controls surrounding the data and communications between TCDRS and the county or district. Accordingly, the list below does not purport to be and is not a complete listing of the control activities that provide a basis for an opinion of the financial statements of the county or district.

Control Objective 1: Census Reports and Accounting Valuation Process

- User organizations are responsible for establishing controls to help ensure that only authorized personnel have permission to access data-related functions on the TCDRS website. This includes:
  - Current and historical employee data (found on the Member Listing report)
  - New employee enrollment (found on the New Member Listing report)
  - Payroll processing and submission (found on the Employer Account Statement or Transaction History page)
- User organizations are responsible for establishing controls to help ensure that only designated personnel maintain documentation regarding plan provisions and help ensure that any plan changes are submitted to TCDRS by their due date (found on the Web Access report).
- User organizations are responsible for establishing controls to help ensure that information provided to TCDRS by authorized personnel is accurate, complete and in accordance with plan guidelines. This includes:
  - Employee enrollment data (found on the New Member Listing report)
  - Employee demographic data, such as name, date of birth and gender
  - Payroll files (found on Transaction History page)
  - Employee eligibility data
  - Employee termination data (found on Employee Termination page, Termination History download).

Control Objective 2: Contributions

- User organizations are responsible for establishing controls to help ensure that only authorized personnel have access to the payroll function on the TCDRS website (found on the Web Access report).
- User organizations are responsible for establishing controls to help ensure that payroll amounts included in payroll files submitted to TCDRS are complete and accurate.
- User organizations are responsible for establishing controls to help ensure that contribution amounts on the TCDRS website are accurate (found on the Employer Account Statement). This includes:
  - Employee deposits
  - Employer contributions
  - Group Term Life premiums (if applicable)

- User organizations are responsible for establishing controls to help ensure that transactions posted to the employer account, as listed on the Employer Account Statement located on the TCDRS website, have been reviewed and confirmed.

Control Objective 5: Distributions

- User organizations are responsible for establishing controls to help ensure that only appropriate personnel provide termination dates for exiting employees on the website (found on the Web Access report).

Control Objective 7: Logical Access

- User organizations are responsible for establishing controls to help ensure that Access to personal computers and terminals is limited to authorized and appropriate personnel.
- User organizations are responsible for establishing controls to help ensure that the designated Security Administrator regularly reviews which individuals have access to the TCDRS website.

Complementary Sub-Service Organization Controls

TCDRS uses a subservice organization to perform some of the services provided to user entities, which are not included in the scope of this report. The TCDRS system was designed with the assumption that certain control objectives can be achieved only if complementary subservice organization controls (CSOC) assumed in the design of TCDRS controls are suitably designed and operating effectively, along with the related controls of TCDRS. The subservice organizations and the respective CSOCs are described in the table below. The CSOCs presented below should not be regarded as a comprehensive list of all of the controls that should be employed by the subservice organizations.

Subservice Organization(s)	Services Provided	Complementary Sub-Service Organization Controls	Control Objective Reference
Data Foundry	Data center hosting	Data Foundry should have controls in place to help ensure that physical access to its data centers are restricted to properly authorized individuals and environmental controls are in place to protect computing resources and equipment.	All
ThreatMetrix	Online risk ratings	ThreatMetrix should have controls in place to restrict system resource access to properly authorized individuals. ThreatMetrix should have controls in place to help ensure data is protected and encrypted at rest and in transit. ThreatMetrix should have controls in place to help ensure the infrastructure remains secure and active monitoring is conducted to identify any risk or abnormal activity or exposure. ThreatMetrix should have controls in place to monitor job schedules and identify and resolve deviations in a complete, accurate, and timely manner. ThreatMetrix should have controls in place to regularly back up data and maintain it for restoration. ThreatMetrix should have controls in place to schedule and monitor the completion of data transmissions. ThreatMetrix should have controls in place to help ensure that physical access to its data centers are restricted to properly authorized individuals and environmental controls are in place to protect computing resources and equipment.	5
Plaid	Online bank account verification	Plaid should have controls in place to help ensure data is protected and encrypted at rest and in transit. Plaid should have controls in place to help ensure changes to program and data are authorized, tested and approved.	5
Okta	Password reset	Okta should have controls in place to restrict system resource access to properly authorized individuals. Okta should have controls in place to help ensure changes to program and data are authorized, tested and approved.	7

Section IV.

Texas County & District Retirement System's Control Objectives, Related Controls, and KPMG LLP's Test of Controls and Results

KPMG Test Procedures

KPMG's tests of the effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls were sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved throughout the period covered by this report. In selecting particular tests of the operating effectiveness of controls, the following were considered: (a) the nature of the items being tested; (b) the types and competence of available evidential matter; (c) the nature of the control objectives to be achieved; and (d) the expected efficiency and effectiveness of the test. Our procedures included inquiry of management, supervisory, and staff personnel; inspection of documents and records; and observation of activities and operations and test of controls related to the commodity risk management application and related application support services for the period May 1, 2023 to April 30, 2024.

In addition, when using information produced by TCDRS, our procedures included an evaluation of the reliability of such information for our purposes by obtaining evidence about its completeness and accuracy.

Business Process Controls

Census Reports and Accounting Valuation Process

Control Objective 1: Controls provide reasonable assurance that reporting of participant census and accounting valuation data to the TCDRS outside actuary is complete and accurate.			
Control Number	**Description of Controls**	**Testing Performed by KPMG LLP**	**Results of Testing**
1.01	Compass enforces valid date of birth entries for new member enrollment.	Observed an attempt to enroll a new member through the web new member form with an invalid date of birth and determined an exception case was created in Compass. Observed an attempt to enroll a new member through a web file upload with a mismatched date of birth and determined an exception case was created in Compass.	No exceptions noted.
1.02	Employer Services traces the employer representative who signed the plan change authorization to the list of authorized employer representatives before processing the plan change.	Inspected the plan agreement and the designated list of authorized employer representatives in Compass for a selection of plan changes and determined plan changes were approved by an authorized employer representative.	No exceptions noted.
1.03	A separate EPM employee performs a review of plan changes to help ensure the accuracy of the change made in Compass.	Inspected the Plan Change case files in Compass for a selection of plan changes and determined a separate EPM employee performed a review of the change to ensure accuracy.	No exceptions noted.
1.04	EPM reviews exception reports to help ensure the completeness and accuracy of member data, deposit transactions, service credit, member balances and interest, effective dates, account statuses, and contribution reports prior to creation of the valuation file.	Inspected the exception reports and emails confirming the completion of the review of the exception reports and determined the review of completeness and accuracy of the valuation file was completed by EPM.	No exceptions noted.

Control Objective 1: Controls provide reasonable assurance that reporting of participant census and accounting valuation data to the TCDRS outside actuary is complete and accurate.			
Control Number	**Description of Controls**	**Testing Performed by KPMG LLP**	**Results of Testing**
1.05	Actuarial Services personnel reconcile the employers in the plan data file for the current year to independent queries from the tEDS data warehouse to validate the completeness and accuracy of the plan data file. In addition, Actuarial Services personnel reconcile the member and retiree data in the member and annuitant files, respectively, for the current year to independent queries from the tEDS data warehouse to validate the completeness and accuracy of the member and annuitant files.	Inspected the reconciliation of new plans and employers in the plan data file to queries from the tEDS data warehouse and determined Actuarial Services personnel performed the review over completeness and accuracy of the file.	No exceptions noted.
		Inspected the reconciliation of member and retiree data in the member and annuitant files to queries from the tEDS data warehouse and determined Actuarial Services personnel performed the review over completeness and accuracy of the file.	No exceptions noted.
1.06	Each year, the Director of Finance reconciles the total employer amounts in the “Changes in Employees Saving Fund (ESF) File” submitted with the valuation file to the amounts captured in Dynamics GP to help ensure the “Changes in ESF File” is recorded completely and accurately.	Inspected the reconciliation of the “Changes in ESF File” and determined the Director of Finance performed the review over completeness and accuracy of the file.	No exceptions noted.
		Inspected the total employer amounts in the “Changes in ESF File” submitted with the valuation file and inspected the amounts in Dynamics GP and determined the amounts agreed.	No exceptions noted.
1.07	The Director of Finance reconciles the total employer amounts in the “Changes in Subdivision Accumulation Fund (SAF) File” submitted with the valuation file to the amounts captured in Dynamics GP to help ensure the “Changes in SAF File” is recorded completely and accurately.	Inspected the reconciliation of the “Changes in SAF File” and determined the Director of Finance performed the review over completeness and accuracy of the file.	No exceptions noted.
		Inspected the total employer amounts in the “Changes in SAF File” submitted with the valuation file and inspected the amounts in Dynamics GP and determined the amounts agreed.	No exceptions noted.

Control Objective 1: Controls provide reasonable assurance that reporting of participant census and accounting valuation data to the TCDRS outside actuary is complete and accurate.			
Control Number	**Description of Controls**	**Testing Performed by KPMG LLP**	**Results of Testing**
1.08	Actuarial Services compares plan assets, benefit plan provisions and member and retiree record counts in the valuation results received from the consulting actuary to the data provided by TCDRS to verify their accuracy and consistency and ensures that the results were uploaded into Compass completely and accurately.	Inspected the verification checklist and supporting documentation and determined that Actuarial Services compared plan assets, benefit plan provisions and retiree record counts in the valuation results received from the consulting actuary to the data provided by TCDRS to verify their accuracy and consistency, as well as verified that the results were uploaded in Compass completely and accurately.	No exceptions noted.

Contributions

Control Objective 2: Controls provide reasonable assurance that contributions received from employers are completely and accurately posted to the employee and employer accounts.			
Control Number	**Description of Controls**	**Testing Performed by KPMG LLP**	**Results of Testing**
2.01	EPM reviews exception reports and resolves contributions where the contribution amounts received exceed thresholds.	Inspected the review of exception reports for a selection of months and determined that the reports were reviewed by EPM and contributions where the contribution amounts exceeded thresholds were investigated and resolved.	No exceptions noted.
2.02	EPM reviews the monthly "No Employer Deposit by Month" report to investigate and resolve employers whose contributions have not been processed in Compass.	Inspected the "No Employer Deposit by Month" report review for a selection of months and determined the report was reviewed by EPM to investigate and resolve employers whose contributions had not been processed in Compass.	No exceptions noted.
2.03	Compass validates matching SSN during the upload employee contribution process and denies processing files until validations are corrected. Contributions received for closed accounts are treated as exceptions cases if received more than a month after termination, or if more than two deposits are received within one month after termination. Exception cases are resolved by Employer Plan Management.	Observed an attempt to upload an employee contribution file with an employee for an unmatched SSN in Compass and determined the upload was denied until the error was corrected.	No exceptions noted.
		Observed an attempt to upload a third contribution for an employee with an account closed less than a month in Compass and determined an exception case was created.	No exceptions noted.
		Observed an attempt to upload a contribution for an employee with an account closed more than a month in Compass and determined an exception case was created.	No exceptions noted.
		Inspected a selection of exception cases and determined they were resolved.	No exceptions noted.

Control Objective 2: Controls provide reasonable assurance that contributions received from employers are completely and accurately posted to the employee and employer accounts.			
Control Number	**Description of Controls**	**Testing Performed by KPMG LLP**	**Results of Testing**
2.04	The Finance team reviews the "Receivable Documents" report at least weekly to help ensure invoices are correct with no duplicates and payments are accurately applied to employer reported amounts.	Inspected the "Receivable Documents" report review for a selection of weeks and determined the Finance team maintained and reviewed the report to help ensure invoices are correct with no duplicates and payments are accurately applied to employer reported amounts.	No exceptions noted.
2.05	Finance staff performs monthly reconciliations of contributions funds recorded in Dynamics GP with the monthly bank statement and the reconciliation is reviewed by a separate person in Finance.	Inspected a selection of monthly reconciliations of contributions funds received and determined they were prepared and reviewed by separate individuals in Finance.	No exceptions noted.
2.06	Compass forces contribution files received and processed by Employer Plan Management to match the total amount entered by the employer in the Employer Portal. Dynamics Great Plains automatically creates the receivable based on this amount.	Observed an attempt to process a contribution file containing a total contribution amount not equal to the amount entered by the employer in the Employer Portal and determined the system generated an error and the file was not processed.	No exceptions noted.
		Observed the entry of the total contribution amount in the Employer Portal and determined that a corresponding receivable in Dynamics Great Plains was created for the same amount.	No exceptions noted.
2.07	The Accounting and EPM departments approve the ACH debit amount prior to debiting the employer accounts.	Inspected a selection of ACH debits and inspected approvals from the Accounting and the EPM departments and determined both groups approved the ACH debit.	No exceptions noted.
2.08	Individuals with access to create and load the ACH debit file do not have access permissions to also release ACH debit files.	Inspected access rights at the bank to create and release an ACH debit file and determined individuals were restricted from having rights to both create and release an ACH debit file.	No exceptions noted.

Income Allocations

Control Objective 3: Controls provide reasonable assurance that income allocations are completely and accurately posted to employer and employee accounts based on amounts approved by the Board of Trustees.			
Control Number	**Description of Controls**	**Testing Performed by KPMG LLP**	**Results of Testing**
3.01	The Board of Trustees approves the allocation rate to apply to SAF balances based on investment returns and executive recommendations.	Inspected the Board of Trustees minutes from the meeting and determined the allocation rate was formally approved.	No exceptions noted.
3.02	Actuarial Services reviews the spreadsheet used to allocate net investment income to employers to help ensure the calculations are accurate and amounts allocated match those approved by the Board of Trustees.	Inspected the allocation working file to determine if all values were properly calculated using the rate approved by the Board of Trustees and determined the calculations were accurate.	No exceptions noted.
		Inspected the recalculation of employer allocation and determined Actuarial Services performed a review to confirm the accuracy of the amounts.	No exceptions noted.
3.03	Annually, the Member Benefits lead and the EPM manager perform a review of ESF interest applied to all member accounts to verify Compass has applied interest accurately within the established thresholds.	Inspected the review of ESF interest applied to all member accounts and determined it was completed by the Member Benefits lead and the EPM manager and discrepancies were investigated and resolved to help ensure the accuracy of interest applied to all member accounts.	No exceptions noted.
3.04	The calculation to allocate funds (i.e., available income or loss) to the General Reserve is reviewed annually for completeness and accuracy by the Director of Finance.	Inspected the allocation worksheet and accompanying checklist and determined the Director of Finance reviewed the worksheet and confirmed net investment income was completely and accurately allocated between SAF and the General Reserve.	No exceptions noted.

Fund Balances

Control Objective 4: Controls provide reasonable assurance that fund balances are reconciled and reported accurately and completely.			
Control Number	**Description of Controls**	**Testing Performed by KPMG LLP**	**Results of Testing**
4.01	Annually, the Director of Finance reconciles the total employer amounts in the "Changes in ESF" file submitted with the valuation file to the amounts captured in Dynamics GP to help ensure the "Changes in ESF" file is complete and accurate.	Inspected the reconciliation of the "Changes in ESF File" and determined the Director of Finance performed the review over completeness and accuracy of the file.	No exceptions noted.
		Inspected the total employer amounts in the "Changes in ESF File" submitted with the valuation file and inspected the amounts in Dynamics GP and determined the amounts agreed.	No exceptions noted.
4.02	Annually, the Director of Finance reconciles the total employer amounts in the "Changes in SAF" file submitted with the valuation file to the amounts captured in Dynamics GP to help ensure the "Changes in SAF" file is complete and accurate.	Inspected the reconciliation of the "Changes in SAF File" and determined the Director of Finance performed the review over completeness and accuracy of the file.	No exceptions noted.
		Inspected the total employer amounts in the "Changes in SAF File" submitted with the valuation file and inspected the amounts in Dynamics GP and determined the amounts agreed.	No exceptions noted.
4.03	Annually, the Director of Finance reviews the worksheet supporting the change in Endowment and Expense funds to help ensure the funds are reviewed prior to sending to the outside actuary.	Inspected the worksheet supporting the change in Endowment and Expense funds and determined the Director of Finance reviewed the worksheet to ensure the fund balances are accurate.	No exceptions noted.

Distributions

Control Objective 5: Controls provide reasonable assurance that distributions (i.e., disability, partial lump sum, withdrawals, and service retirements) are authorized and processed accurately and completely.			
Control Number	**Description of Controls**	**Testing Performed by KPMG LLP**	**Results of Testing**
5.01	Access to post payments in Dynamics GP is restricted to Accounting personnel.	Inspected the organizational chart and the system list of users with access to post payments in Dynamics GP and determined access is restricted to Accounting personnel.	No exceptions noted.
5.02	Access to Compass is restricted as follows: • The permissions to process distributions in Compass are restricted to Member Benefits and Member Services personnel and a designated backup. • The permissions to process contributions are restricted to EPM personnel.	Inspected the organizational chart and the system list of users with the permissions in Compass to process benefit distributions and determined access is restricted to Member Benefits and Member Services personnel and a designated backup.	No exceptions noted.
		Inspected the organizational chart and the system list of users with permissions in Compass to process contributions and determined access is restricted to EPM personnel.	No exceptions noted.
5.03	Annually, the Member Benefits lead and the EPM manager perform a review of ESF interest applied to all member accounts to verify Compass has applied interest accurately within the established thresholds.	Inspected the annual review of ESF interest applied to all member accounts and determined it was completed by the Member Benefits lead and the EPM manager and discrepancies were investigated and resolved to help ensure the accuracy of interest applied to all member accounts.	No exceptions noted.
5.04	Member Services performs a QA of annuity and partial lump sum calculations at least annually to help ensure the payments are accurately calculated.	Inspected the Retirement Benefit Calculation worksheet and supporting documentation for an annuity and a partial lump sum payment and determined Member Services recalculated the distributions for accuracy as part of QA.	No exceptions noted.

Control Objective 5: Controls provide reasonable assurance that distributions (i.e., disability, partial lump sum, withdrawals, and service retirements) are authorized and processed accurately and completely.			
Control Number	**Description of Controls**	**Testing Performed by KPMG LLP**	**Results of Testing**
5.05	The Accounting department reconciles retirement transfers from ESF to SAF and ongoing annuity payment amount activity in Compass and Dynamics GP on a monthly basis.	Inspected a selection of monthly reconciliations of retirement transfers and ongoing annuity payments and determined the reconciliations were performed and reconciling items were investigated and tracked for resolution purposes.	No exceptions noted.
5.06	System edit checks prevent unauthorized partial lump sum payments by enforcing the following edits: • System validation prevents partial lump sum payment entries unless authorized as a plan provision by the employer. • System validation prevents a partial lump sum payment amount from exceeding the amount available in the member's account balance. • System validation automatically reduces the monthly benefit calculation by the partial lump sum payment processed. • System validation requires an electronic signature to process the partial lump sum payments	Observed an attempt in Compass to issue a partial lump sum payment for a plan that did not elect for this form of distribution and determined the payment was denied.	No exceptions noted.
		Observed an attempt in Compass to issue a partial lump sum payment for an amount exceeding the member's balance and determined the payment was denied.	No exceptions noted.
		Inspected the benefit calculations in Compass for a member receiving a monthly benefit and a partial lump sum payment and determined the reserves for the monthly benefit are reduced by the partial lump sum payment.	No exceptions noted.
		Observed an attempt in Compass to issue a partial lump sum payment and determined that an electronic signature was required to process the partial lump sum payments.	No exceptions noted.
5.07	For withdrawal applications submitted by paper, Compass is configured to require a Member Benefits Analyst to confirm the proof of member identity and member-signed withdrawal form prior to processing a withdrawal.	Observed an attempt to process a withdrawal in Compass without noting the confirmation of the proof of member identity and the member-signed withdrawal form in the required Compass field and determined confirming proof of member identity and receipt of member-signed withdrawal form was required prior to processing.	No exceptions noted.

Control Objective 5: Controls provide reasonable assurance that distributions (i.e., disability, partial lump sum, withdrawals, and service retirements) are authorized and processed accurately and completely.			
Control Number	**Description of Controls**	**Testing Performed by KPMG LLP**	**Results of Testing**
5.08	An annual review is conducted on all death cases for which a user with the ability to conduct the quality assurance review performed a review of their own case. Any such cases identified are investigated and resolved.	Inspected the annual death case review and determined that all death cases for which a user with the ability to conduct the quality assurance review performed a review of their own case were investigated and resolved.	No exceptions noted.
5.09	Member Services updates member records based on reviews of death matches from Texas Department of Vital Statistics (monthly) and PBI (weekly) to detect member deaths that were not previously reported.	Inspected a selection of monthly Texas Department of Vital Statistics (TVS) reports and determined that death matches were reviewed by Member Services. For selection of records on the TVS reports, inspected Compass screens and determined the death matches were accurately updated.	No exceptions noted.
		Inspected a selection of weekly PBI reports and determined that death matches were reviewed by Member Services. For selection of records on the PBI reports, inspected Compass screens and determined the death matches were accurately updated.	No exceptions noted.
5.10	Annually, Member Services detects and resolves inaccurate and incomplete COLA updates (including CPI adjustments) by reviewing the COLA Verification report prior to processing any benefit payment changes.	Inspected the annual COLA Verification report review and determined Member Services reviewed the reports and resolved inaccurate and incomplete COLA updates prior to processing any benefit payment changes.	No exceptions noted.
5.11	Member Services reviews the Annuity Change Report to identify annuity changes exceeding $30 on a monthly basis. Changes exceeding $30 are investigated and approved.	Inspected the Annuity Change Report for a selection of months and determined Member Services identified, investigated and approved changes exceeding $30.	No exceptions noted.

Control Objective 5: Controls provide reasonable assurance that distributions (i.e., disability, partial lump sum, withdrawals, and service retirements) are authorized and processed accurately and completely.			
Control Number	**Description of Controls**	**Testing Performed by KPMG LLP**	**Results of Testing**
5.12	Access to process employee terminations in the Employer Portal is restricted to users with the Benefits or Security Admin roles.	Observed an attempt to process an employee termination in the Employer Portal with roles other than Benefits and Security Admin roles and determined only the Benefits and Security Admin roles have access to process employee terminations.	No exceptions noted.
		Observed an attempt to change the termination date for a member in Compass and determined the field was not editable within the Compass workflow.	No exceptions noted.
5.13	Access to assign new county and district security administrators in the Employer Portal is restricted to the TCDRS Employer Services team and authorized IT personnel via the "InternalPortalEmployerServices" and “InternalPortalAdministrators” Active Directory groups.	Inspected the organizational chart and the "InternalPortalEmployerServices" and “InternalPortalAdministrators” Active Directory groups and determined the users were restricted to TCDRS Employer Services and authorized IT personnel.	No exceptions noted.
5.14	Prior to processing terminations, the Employer Portal requires the SSN matches an existing member in Compass and benefits have not been previously processed.	Observed an attempt to process a termination with an SSN that doesn't exist in Compass and determined an error message was generated and the termination could not be processed.	No exceptions noted.
		Observed an attempt to process a termination for an employee already receiving benefits and determined an error message was generated and the termination could not be processed.	No exceptions noted.

Control Objective 5: Controls provide reasonable assurance that distributions (i.e., disability, partial lump sum, withdrawals, and service retirements) are authorized and processed accurately and completely.			
Control Number	**Description of Controls**	**Testing Performed by KPMG LLP**	**Results of Testing**
5.15	The Account Balance Exceptions report is generated by Member Services on at least a monthly basis to investigate and resolve closed member accounts with a positive or negative balance.	Inspected the Account Balance Exceptions report review for a selection of months and determined Member Services investigated and resolved closed member accounts with a positive or negative balance.	No exceptions noted.
5.16	On a monthly basis, the Annuity Account Status Validation report is generated by Member Services to investigate and resolve instances in which a deceased member has an open annuity account.	Inspected the Annuity Account Status Validation report review for a selection of months and determined Member Services investigated and resolved open annuity accounts for deceased members.	No exceptions noted.
5.17	For retirements and payment address updates submitted online or over the phone, an Anti-Fraud Analyst investigates and resolves the Security Case created when there is an Authentication Case Failure. Failed authentication occurs when there is either a high Emailage or PhoneFinder fail or a reject ThreatMetrix result (if application originated from the web).	Observed an attempt to process a service retirement in Compass for a member with a low Emailage, a pass PhoneFinder, and a pass ThreatMetrix result and determined the Anti-Fraud Analyst was not required to investigate prior to processing the annuity.	No exceptions noted.
		Observed an attempt to process a service retirement in Compass for a member with a high Emailage, a pass PhoneFinder, and a pass ThreatMetrix result and determined that the Anti-Fraud Analyst investigated and resolved the case.	No exceptions noted.
		Observed an attempt to process a service retirement in Compass for a member with a low Emailage and a fail PhoneFinder result and determined that the Anti-Fraud Analyst investigated and resolved the case.	No exceptions noted.

Control Objective 5: Controls provide reasonable assurance that distributions (i.e., disability, partial lump sum, withdrawals, and service retirements) are authorized and processed accurately and completely.			
Control Number	**Description of Controls**	**Testing Performed by KPMG LLP**	**Results of Testing**
		Observed an attempt to process a service retirement in Compass for a member with a low Emailage, a pass PhoneFinder, and a reject ThreatMetrix result and determined that the Anti-Fraud Analyst investigated and resolved the case.	No exceptions noted.
5.18	For withdrawals submitted online or over the phone, an Anti-Fraud Analyst investigates and resolves the Security Case created when there is an Authentication Case Failure. Failed authentication occurs when there is either an Emailage or PhoneFinder fail or a reject ThreatMetrix result (if application originated from the web).	Observed an attempt to process a withdrawal in Compass for a member with a low Emailage, a pass PhoneFinder, and a pass ThreatMetrix result and determined the Anti-Fraud Analyst was not required to investigate prior to processing the annuity.	No exceptions noted.
		Observed an attempt to process a withdrawal in Compass for a member with a high Emailage and a pass PhoneFinder result and determined that the Anti-Fraud Analyst investigated and resolved the case.	No exceptions noted.
		Observed an attempt to process a withdrawal in Compass for a member with a low Emailage, a fail PhoneFinder result and determined that the Anti-Fraud Analyst investigated and resolved the case.	No exceptions noted.
		Observed an attempt to process a withdrawal in Compass for a member with a low Emailage, a pass PhoneFinder, and a reject ThreatMetrix result and determined that the Anti-Fraud Analyst investigated and resolved the case.	No exceptions noted.

Control Objective 5: Controls provide reasonable assurance that distributions (i.e., disability, partial lump sum, withdrawals, and service retirements) are authorized and processed accurately and completely.			
Control Number	**Description of Controls**	**Testing Performed by KPMG LLP**	**Results of Testing**
5.19	Withdrawal requests under $100,000 in which Authentication Case was a Pass are not reviewed.	Observed an online attempt to process a withdrawal in Compass for a member with an amount under $100,000 and determined the withdrawal was automatically approved and processed accurately.	No exceptions noted.
		Observed an attempt to process a withdrawal in Compass via phone for a member with an amount under $100,000 and determined the withdrawal was automatically approved and processed accurately.	No exceptions noted.
5.20	Withdrawal requests equal to or greater than $100,000 create an exception case that must be acknowledged by Member Benefits Analyst regardless of the Authentication Case results.	Observed an online attempt to process a withdrawal in Compass for a member with an amount equal to or greater than $100,000 and determined the exception case required a review by a Member Benefits Analyst.	No exceptions noted.
		Observed an attempt to process a withdrawal in Compass via phone for a member with an amount equal to or greater than $100,000 and determined the exception case required a review by a Member Benefits Analyst.	No exceptions noted.

Control Objective 5: Controls provide reasonable assurance that distributions (i.e., disability, partial lump sum, withdrawals, and service retirements) are authorized and processed accurately and completely.			
Control Number	**Description of Controls**	**Testing Performed by KPMG LLP**	**Results of Testing**
5.21	Compass is configured to require a termination date to be submitted by the employer prior to disbursing service retirement annuities, disability retirement annuities, or withdrawals, whether submitted online, by paper or by phone.	Observed an attempt to process a service retirement, disability retirement, and withdrawal submitted by paper and determined the system prevented the payments from being disbursed without a termination date entered by the employer.	No exceptions noted.
		Observed an attempt to process a service retirement, disability retirement, and withdrawal submitted online and determined the system prevented the payments from being disbursed without a termination date entered by the employer.	No exceptions noted.
		Observed an attempt to process a service retirement, disability retirement, and withdrawal submitted by phone and determined the system prevented the payments from being disbursed without a termination date entered by the employer.	No exceptions noted.
5.22	Compass is configured to process continued death benefits accurately based on the original retirement option.	Observed an attempt to process continued death benefits for a selection of retirement options and noted the benefits were processed accurately.	No exceptions noted.

Information Technology Controls

Applications Maintenance

Control Objective 6: Controls provide reasonable assurance that modifications to applications are authorized, tested, approved, documented, and implemented.			
Control Number	**Description of Controls**	**Testing Performed by KPMG LLP**	**Results of Testing**
6.01	Application changes are documented and authorized by a Director or Manager from the business area for development by the change management team.	Inspected a selection of changes and the organizational chart and determined changes were authorized by a Director or Manager from the business area for development by the change management team.	No exceptions noted.
6.02	Application changes are tested and approved prior to implementation to the production environment.	Inspected a selection of changes and determined changes were tested and approved prior to implementation in the production environment.	No exceptions noted.
6.03	Access to implement application changes for the Dynamics GP, Compass, Employer Portal and Member Portal environments is restricted to authorized and appropriate personnel based on job responsibility.	Inspected list of users with access to implement changes in production, inspected the organizational chart and inquired of management and determined access is restricted to authorized and appropriate users based on job responsibility.	No exceptions noted.
6.04	Access to production is temporarily granted to enable developers to implement changes once the change is approved.	Inspected the system configuration and determined that access to production was temporarily granted for 18 hours to enable developers to implement changes once the change was approved.	No exceptions noted.
6.05	On a monthly basis, the Deputy Executive Director or Director of Infrastructure and Security performs an access review to help ensure that access was appropriate and aligned with approved deployments.	Inspected a selection of monthly access reviews and determined that the Deputy Executive Director or Director of Infrastructure and Security reviewed that access was appropriate and aligned with approved deployments.	No exceptions noted.

Logical Access

Control Objective 7: Controls provide reasonable assurance that logical access to programs and data is granted to authorized individuals.			
Control Number	**Description of Controls**	**Testing Performed by KPMG LLP**	**Results of Testing**
7.01	Logical access to applications is documented and authorized by HR and the Business Director or designated hiring manager.	Inspected the authorization forms for a selection of applications new users and determined they were approved by HR and the Business Director or designated hiring manager.	No exceptions noted.
7.02	Access to information resources is protected by passwords per policy are configured as follows: Expiration: 60 days Minimum Length: 6 characters Complexity: Required Password history: 5 previous passwords Compass application access is authenticated by TCDRS's internal Active Directory. Dynamics GP application authentication is based on SQL logins which are configured to authenticate using internal Active Directory password configurations. Employer Portal, Member Portal, Customer Service Portal and Back Office portal access is authenticated by internal Active Directory maintained by TCDRS. The Compass, Dynamics GP and tERS databases are configured to authenticate using internal Active Directory password configurations.	Inspected internal Active Directory password settings that enforce passwords to the Compass application and determined they were configured according to policy.	No exceptions noted.
		Inspected Dynamics GP SQL password settings for application users and determined they were configured to have internal Active Directory enforce password configurations.	No exceptions noted.
		Inspected Dynamics GP SQL database password settings and determined they were configured to have internal Active Directory enforce password configurations.	No exceptions noted.
		Inspected external Active Directory password settings that enforce password settings for Employer, Member, Customer Service, and Back Office Portals and determined they were configured according to policy.	No exceptions noted.
		Inspected Compass SQL database password settings and determined they were configured to have internal Active Directory enforce password configurations.	No exceptions noted.

Control Objective 7: Controls provide reasonable assurance that logical access to programs and data is granted to authorized individuals.			
Control Number	**Description of Controls**	**Testing Performed by KPMG LLP**	**Results of Testing**
	Application and database servers are configured to inherit the internal Active Directory password settings. Accounts stored in Privileged Access Management Secret Server are configured as follows: Complexity: Required Minimum Length: 12 characters The virtual host server uses Active Directory for authentication.	Inspected the tERS SQL database password settings and determined they were configured to have internal Active Directory enforce password configurations.	No exceptions noted.
		Inspected the internal Active Directory default domain policy scope and determined that all application and database servers are configured to inherit the internal Active Directory default domain policy password settings.	No exceptions noted.
		Inspected the Privileged Access Management Secret Server password configurations and determined that all accounts stored in Privileged Access Management Secret Server are configured with the following settings enforced: Complexity: Required Minimum Length: 12 characters	No exceptions noted.
		Inspected the virtual server host password setting and determined that the virtual host server uses Active Directory for authentication.	No exceptions noted.

Control Objective 7: Controls provide reasonable assurance that logical access to programs and data is granted to authorized individuals.			
Control Number	**Description of Controls**	**Testing Performed by KPMG LLP**	**Results of Testing**
7.03	Administrative access to application servers and database servers is restricted to authorized individuals based on their job responsibilities.	Inspected the system list of users with administrative access to the following: • Active Directory (internal and external) • Application and database servers for the Dynamics GP, Compass, tERS, Employer Portal and Member Portal applications • Virtual server host Inspected the organizational chart and inquired of management and determined access is restricted to authorized individuals based on their job responsibilities.	No exceptions noted.
7.04	Administrative access to applications and databases is restricted to authorized individuals based on their job responsibilities.	Inspected the system list of users with administrative access to the Dynamics GP application, inspected the organizational chart and inquired of management and determined access was restricted to authorized individuals based on their job responsibilities.	No exceptions noted.
		Inspected the system list of users with administrative access to the Dynamics GP SQL database, inspected the organizational chart and inquired of management and determined access was restricted to authorized users.	No exceptions noted.
		Inspected the system list of users with administrative access to the Compass application, inspected the organizational chart and inquired of management and determined access was restricted to authorized users.	No exceptions noted.

Control Objective 7: Controls provide reasonable assurance that logical access to programs and data is granted to authorized individuals.			
Control Number	**Description of Controls**	**Testing Performed by KPMG LLP**	**Results of Testing**
		Inspected the system list of users with administrative access to the Compass database and tERS database and inquired of management and determined access was restricted to authorized users.	No exceptions noted.
		Inspected the system list of users with administrative access to the Employer and Member Portal, inspected the organizational chart and inquired of management and determined access was restricted to authorized users.	No exceptions noted.
7.05	Terminated users' network, application, operating system, and database accounts are disabled within one business day.	Inspected the tickets corresponding to disabling the employee's account for a selection of terminated employees and inspected a list of network, application, operating system, and database users and determined that the users had been disabled within one business day.	No exceptions noted.
7.06	A semi-annual review of Compass, Employer Portal, Member Portal, ThreatMetrix, Okta, JPMorgan, and Plaid accounts is performed by Directors.	Inspected two instances of the semi-annual review of Compass, Employer Portal, Member Portal, ThreatMetrix, Okta, JPMorgan, and Plaid accounts and determined users and privileges were reviewed and approved by Directors and any discrepancies resolved.	No exceptions noted.
7.07	A quarterly review of database accounts for Dynamics GP, Compass and tERS is performed by Directors.	Inspected the review of database accounts for a selection of quarters and determined users and privileges were reviewed and approved by Directors and any discrepancies resolved.	No exceptions noted.

Control Objective 7: Controls provide reasonable assurance that logical access to programs and data is granted to authorized individuals.			
Control Number	**Description of Controls**	**Testing Performed by KPMG LLP**	**Results of Testing**
7.08	A monthly review of privileged domain accounts is performed by Directors.	Inspected the review of privileged domain accounts for a selection of months and determined users and privileges were reviewed and approved by Directors and any discrepancies resolved.	No exceptions noted.
7.09	An annual review of Dynamics GP application accounts is performed by Directors.	Inspected the annual review of Dynamics GP application accounts and determined the accounts were reviewed and approved by management and any discrepancies resolved.	No exceptions noted.
7.10	Firewalls are used to limit ports available to external users and to limit access to internal computing resources.	Inspected firewall configurations and IPS signature updates and determined firewalls were configured to limit ports available to external users and to limit access to internal computing resources and the IPS patches are updated.	No exceptions noted.
7.11	A quarterly review of firewall rules by an Infrastructure Services security specialist is completed in accordance with the IT Security Policy.	Inspected the review of firewall rules for a selection of quarters and determined firewall rules were reviewed and approved by an Infrastructure Services security specialist in accordance with the IT Security Policy and any discrepancies resolved.	No exceptions noted.
7.12	Administrative access to the Privileged Access Management Secret Server is restricted to authorized individuals based on their job responsibilities.	Inspected the system list of users with administrative access to Privileged Access Management Secret Server and determined access was restricted to authorized users. Inspected the organizational chart and inquired of management and determined access is restricted to authorized individuals based on their job responsibilities.	No exceptions noted.

Backups

Control Objective 8: Controls provide reasonable assurance that data and systems are backed up on a scheduled basis, stored in an offsite location and available for restoration.			
Control Number	**Description of Controls**	**Testing Performed by KPMG LLP**	**Results of Testing**
8.01	Incremental database backups are completed nightly and full database backups are completed weekly.	Inspected database backup schedules and determined incremental data backups are scheduled nightly and full data backups are scheduled weekly.	No exceptions noted.
8.02	Production application and database servers are backed up offsite monthly and transaction logs are backed up every 30 minutes between local production servers.	Inspected server backup schedules and determined production application and database servers were scheduled to backup offsite monthly and transaction logs were scheduled to back up every 30 minutes.	No exceptions noted.
		Inspected backup copies logs for a selection of months and determined that data from local production servers was successfully replicated to the offsite backup appliances.	No exceptions noted.
8.03	Database administrators and Infrastructure Services monitor and resolve backup errors.	Inspected the help desk ticket opened or resolution evidence for a selection of backup errors during the period and to determine whether the failure was recorded and resolved by database administrators or Infrastructure Services.	KPMG was unable to test and conclude on the operating effectiveness of this control as there were no backup errors during the period.
8.04	Access to backup schedulers is limited to database administrators and Infrastructure Services staff.	Inspected the system list of accounts with access to the backup scheduler and inquired of management and determined access was restricted to database administrators and Infrastructure Services staff.	No exceptions noted.

Control Objective 8: Controls provide reasonable assurance that data and systems are backed up on a scheduled basis, stored in an offsite location and available for restoration.			
Control Number	**Description of Controls**	**Testing Performed by KPMG LLP**	**Results of Testing**
8.05	TCDRS backup files are replicated at an offsite backup facility that provides weekly recovery assurance logs to help ensure offsite backup files are available for restoration.	Inspected recovery assurance logs for a selection of weeks and determined that the data and system files were available to be restored.	No exceptions noted.