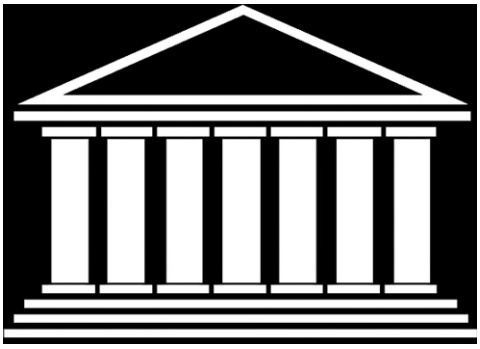


The Resource Centers, LLC

SOC 1 Type 2

Independent Service Auditor's Report on Management's Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls

October 1, 2021 – September 30, 2022

200 Second Avenue South, Suite 478
St. Petersburg, FL 33701

TABLE OF CONTENTS

I. Independent Service Auditor's Report ***3***

Independent Service Auditor's Report **4**

II. Information Provided by The Resource Centers, LLC ***7***

Management Assertions Letter **8**

Description of Relevant Controls Provided by The Resource Centers, LLC **10**

Company Overview 10

Relevant Aspects of the Control Environment, Risk Assessment, Monitoring, and Information and Communication **12**

Control Environment 12

Risk Assessment 16

Monitoring 16

Information and Communication 17

User Control Considerations 25

III. Information Provided by Ascend Audit & Advisory ***26***

Control Objectives, Related Controls, and Tests of Operating Effectiveness **27**

Control Objective 1 – Organization and Administration 27

Control Objective 2 – Information Security: Physical and Logical Access 29

Control Objective 3 – Environmental Security 31

Control Objective 4 – Risk Management 32

Control Objective 5 – Data Backup and Recovery 33

Control Objective 6 – Computer Operations 34

Control Objective 7 – Change Management 37

Control Objective 8 – Pension Benefits Payments 38

Control Objective 9 – Client Reconciliation and Reporting 40

Control Objective 10 – Client Administration 41

I. Independent Service Auditor's Report

200 Second Avenue South, Suite 478
St. Petersburg, FL 33701
www.ascendaudit.com

INDEPENDENT SERVICE AUDITOR'S REPORT

J. Scott Baur
Managing Partner
The Resource Centers, LLC
4360 Northlake Boulevard, Suite 2016
Palm Beach Gardens, FL 33410

Scope

We have examined The Resource Centers, LLC's ("Resource Centers" or "the Company") description of its information technology and pension processing system for processing user entities' transactions throughout the period October 1, 2021 to September 30, 2022 and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

The Resource Centers, LLC's Responsibilities

In Section II of this report, the Company provided an assertion about the fair presentation of the description and the suitability of design and operating effectiveness of the controls to achieve the related control objectives stated in the description. The Company is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the 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; and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Ascend Audit & Advisory's 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. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period October 1, 2021 to September 30, 2022.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description 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 those controls to achieve the related control objectives stated in the description. Our procedures included 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. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described beginning in Section II. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions 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 is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the criteria described in the Company's assertion in Section II of this report,

a. The description fairly presents the information technology and pension processing system that was designed and implemented throughout the period October 1, 2021 to September 30, 2022.

b. 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 October 1, 2021 to September 30, 2022, and user entities applied the complementary user entity controls contemplated in the design of the Company's controls throughout the period October 1, 2021 to September 30, 2022.

c. The controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period October 1, 2021 to September 30, 2022.

Description of Tests of Controls

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

Restricted Use

This report and the description of tests of controls and results thereof in Section III of this report are intended solely for the information and use of the Company, user entities of the Company's information technology and pension processing system throughout the period October 1, 2021 to September 30, 2022, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about the controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Ascend Audit & Advisory

October 17, 2022

II. Information Provided by The Resource Centers, LLC

MANAGEMENT ASSERTIONS LETTER

We have prepared the description of The Resource Centers, LLC's information technology and pension processing system ("description") for user entities of the system throughout the period October 1, 2021 to September 30, 2022, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm to the best of our knowledge and belief, that:

a. The description fairly presents the information technology and pension processing system made available to user entities of the system throughout the period October 1, 2021 to September 30, 2022 for processing their transactions. 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 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 services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information prepared for user entities.

      3) The related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report 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 significant events and conditions, other than transactions.

      5) The process used to prepare reports and other information for user entities.

      6) The specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls contemplated in the design of Resource Center's controls.

      7) Other aspects of the control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.

   ii. Does not omit or distort information relevant to the scope of information technology and pension processing system, while acknowledging that the description is presented to meet the common needs of a broad range of user entities of the system and their financial statement auditors, and may not, therefore, include every aspect of the information technology and pension processing system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. The description includes relevant details of changes to the service organization's system during the period covered by the description when the description covers a period of time.

c. The controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period October 1, 2021 to September 30, 2022 to achieve those control objectives. 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,

   ii. The controls identified in the description would, if operating as described, 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, and manual controls were applied by individuals who have the appropriate competence and authority.

By: /S/ J. Scott Baur

J. Scott Baur
Managing Partner

October 17, 2022

DESCRIPTION OF RELEVANT CONTROLS PROVIDED BY THE RESOURCE CENTERS, LLC

Company Overview

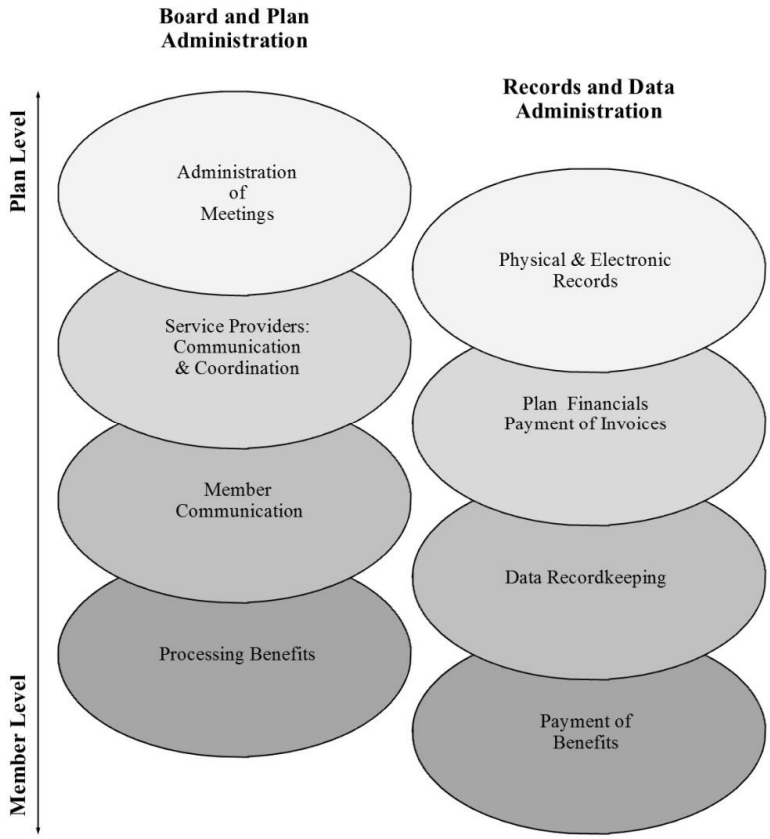
Established in 1996, The Resource Centers has grown to become one of the largest providers of plan administration services and technology solutions to public sector plans. The firm has distinct organizational units for the different products and services. The Resource Centers serves a diverse mix of plans and Boards, and the plans and Boards each come with their own operational constraints.

The Resource Centers team remains committed to the core values of service, integrity, and excellence. Corporate offices support the administration of over 60 public pension plans, a more diverse mix of plans and plan requirements than any other administrator. These plans include over $8 Billion in assets with 15,800 active plan members and 15,000 retirees. The plans collectively make over $30 Million in benefit payments to the 15,000 retired members and their beneficiaries each month.

Products and Services Overview

The Resource Centers provides plan administration services for pensions and benefits in the public sector, the private sector, and multi-employer environment. The Resource Centers also delivers technology solutions to other plan administrators to manage pension and benefit plans more effectively. The Company also offers iRetire, a comprehensive Web-based plan administration portal that incorporates an open architecture in the system design.

The following diagram captures the broad spectrum of tasks required for the administration of a public plan, from the level of the plan down to the individual member, both on the people side and the information side of operations:



Resource Centers provides the following services related to the administration of public defined pension and benefit plans:

- Services Related to Meetings of Trustees
- Services Related to Administration of Board
- Basic Communication
- Plan and Policy Changes
- Coordination of Service Providers
- Review of Statements and Documents
- Public Records Custodian

Resource Centers also offers the following additional services specific to the administration of public pension plans.

Database, Recordkeeping, Systems, and Online Access:

- Maintain Data for Benefit Eligibility of Participants
- Maintain Participant Service, Payroll, and Contribution Data
- Prepare Member Schedules for Annual Audits, State and Actuarial
- Online Access and Benefit Calculation Systems

Benefit Processing:

- Provide Benefit Calculations and Estimates to Members
- Process Member Applications for Other Benefits and Changes
- Assist in Processing Benefit Claims and Appeal

DROP, Share, and Member Accounts and Statements:

- Provide Monthly, Quarterly, or Annual Account Statements to Members
- Provide Online Account Access

Interim Plan Financial Statements:

- Reconcile Local Checking and Custodial Accounts
- Process Accounts Payable
- Monitor and Reconcile Contributions and Deposits
- Review and Reconcile Basic Investment Activity
- Maintain Detail General Ledger of Transactions
- Provide Interim Financial Statements to Applicable Generally Accepted Accounting Principles (GAAP) and Governmental Accounting Standards Board (GASB) Standards

Benefit Payments and Distributions:

- Process Benefit Payments and Distributions
- Track Changes to Payments
- Pay Benefits by Check or ACH Deposit
- Withhold Taxes and Deductions
- Provide All Necessary Reports and Filings for Taxes and Deductions
- Complete Periodic Death Searches of Plan Beneficiaries

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

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. The control environment has a pervasive influence on the structure of business activities, establishment of objectives, and assessment of risks. It influences control activities, information and communication systems, and monitoring procedures. The control environment is influenced by an entity's history and managerial culture. Effectively controlled entities strive to have competent personnel, instill an enterprise-wide attitude of integrity and control consciousness, and set a positive corporate direction. These entities establish appropriate controls that foster shared values and teamwork in pursuit of the organization's objectives.

Control environment elements include the following, and the extent to which each element is addressed at Resource Centers is described below:

- Management Controls, Philosophy, and Operating Style
- Integrity and Ethical Values
- Organizational Structure
- Assignment of Authority and Responsibility
- Standard Operating Controls
- Audit
- Risk Management
- Monitoring

Management Controls, Philosophy, and Operating Style

Management is responsible for directing and controlling operations; establishing, communicating, and monitoring control policies and procedures; and setting the tone for the organization. Importance is placed on accuracy and integrity, maintaining written and updated procedures, security and privacy, and establishing and maintaining sound internal controls over all functional aspects of operations.

Management's philosophy and operating style affect the way the entity is managed, including the kinds of business risks accepted. Resource Centers places a great deal of importance on working to ensure that the integrity of processing is a primary focus and that controls are maximized to mitigate risk in daily operations. Management and specific teams are structured to ensure the highest level of integrity and efficiency in customer support and transaction processing.

Formal job descriptions, regular departmental meetings and staff interactions ensure communication of organizational values, ethics, and behavior standards. Personnel operate under Resource Centers' policies and procedures, including confidentiality agreements and security policies. Periodic training is conducted to communicate regulations and the importance of privacy and security. Management is committed to being aware of regulatory and economic changes that impact lines of business and monitoring the client base for trends, changes, and anomalies. Competence should reflect the knowledge and skills needed to accomplish tasks that define an individual's job. Through consideration of an entity's objectives and the strategies and plans for achievement of those objectives, management must determine how well these tasks need to be accomplished. Management has identified the competence levels for particular jobs and translated those levels into requisite knowledge and skills.

Integrity and Ethical Values

Maintaining a climate that demands integrity and ethical values is critical to the establishment and maintenance of an effectively controlled organization. The effectiveness of internal controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Resource Centers has programs and policies designed to promote and ensure integrity and ethical values in its environment.

Resource Centers desires to maintain a safe, pleasant, and cooperative working environment and expects employees to have high standards of performance, integrity, productivity, and professionalism. Resource Centers has developed professional conduct policies that set forth policies of importance to all employees relating to ethics, values, and conduct. All employees are expected to know and adhere to these standards, as well as to generally accepted norms of conduct and courtesy at all times. While managers are responsible for understanding, communicating, and enforcing Company policies, this does not override or diminish an employee's individual responsibility to be aware of and adhere to these policies. Violations of these policies or other forms of misconduct may lead to disciplinary or corrective action up to and including dismissal.

Standards of Conduct

The Company has implemented standards of conduct to guide all employee and contractor behavior. Management monitors behavior closely, and exceptions to these standards lead to immediate corrective action as defined by Human Resources (HR) policies and procedures. Additionally, all employees must sign confidentiality agreements prior to employment. Any employee found to have violated Resource Centers' ethics policy may be subject to disciplinary action, up to and including termination of employment.

Commitment to Competence

The Company has formal job descriptions that define roles and responsibilities and the experience and background required to perform jobs in a professional and competent fashion. The Company analyzes the knowledge and skills needed to perform job duties and responsibilities and hires for that skill set and job requirement. Management monitors employee and contractor performance and formally evaluates it on a periodic basis to determine that standards are met or exceeded.

Organizational Structure

An entity's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Significant aspects of establishing a relevant organizational structure include defining key areas of authority and responsibility and establishing appropriate lines of reporting. Significant cross-training between management positions and between staff positions exists to help ensure smooth operations and maintenance of controls during staff or management absence.

Assignment of Authority and Responsibility

The extent to which individuals recognize that they are held accountable influences the control environment. This holds true for everyone who has ultimate responsibility for activities within an entity, including the internal control system. This includes assignment of authority and responsibility for operating activities and establishment of reporting relationships and authorization protocols. Resource Centers' Management encourages individuals and teams to use initiative in addressing issues and resolving problems. Policies describing appropriate business practices, knowledge and experience of key personnel, and available resources are provided to employees in order to assist them in carrying out their duties.

The Company is led by a team of senior executives that assigns authority and responsibility to key management personnel with the skills and experience necessary to carry out their assignments. Such assignments commonly relate to achieving corporate objectives, oversight of operating functions, and any compliance with applicable regulatory requirements. Open dialogue and individual initiative are encouraged as fundamental parts of the Company's goal to deliver client service.

Resource Centers' Management sends guidance to employees regarding expected levels of integrity, ethical behavior, and competence. Such practices relate to hiring, orientation, training, evaluation, counseling, promotion, compensation, and remedial actions.

Resource Centers has hiring practices that are designed to help ensure that new employees are qualified for their job responsibilities. All applicants pass through an interview process that assesses their qualifications related to the expected responsibility level of the individual.

The Company has formal job descriptions that define roles and responsibilities and the experience and background required to perform jobs in a professional and competent fashion. The Company determines the knowledge and skills needed to perform job duties and responsibilities and hires for that skill set and job requirement. Management monitors and formally evaluates employee and contractor performance on a periodic basis to determine that performance meets or exceeds Company standards.

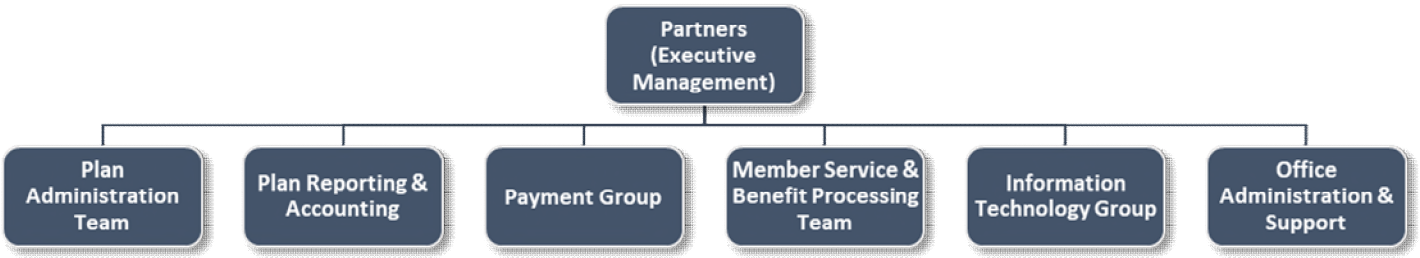
Resource Centers invests significant resources in employee development by providing on-the-job training and other learning opportunities. New employees participate in an informal orientation program that acquaints them with the Company's organization and its functions, values, products, and selected policies. Thereafter, development activities include providing more challenging assignments, job rotation, training programs, seminars, and continuing education programs.

Security Awareness

Each member of Resource Centers is made aware of the security implications that revolve around their functions and actions. Approaching security as an organization has a more profound effect than relying solely on a single group. This process begins with providing individuals with the understanding and knowledge needed to help secure them and their data within established policies. Security awareness programs include the message that individual users can have a significant impact on the overall security of an organization.

Roles and Responsibilities

The following organizational chart depicts Resource Centers' corporate structure.



Partners – Partners oversee the values, vision, organization, function, and personnel for Resource Centers.

Plan Administration Team – This team serves as the primary liaison to client groups, boards, and plan members. Each Plan Administrator is responsible for overall coordination, operation, organization, and administration of assigned plans.

Plan Reporting and Accounting – This team maintains interim financial statements for client plans. An external CPA firm provides qualified management oversight for the production of interim plan financial statements.

Payment Group – This team processes accounts payable and benefits for client plans. This team issues all payments, posts transactions to the general ledger, generates related reports, files tax deposits and documents for benefit payments, maintains member database for death searches, and maintains local client checking accounts.

Member Service and Benefit Processing Team – This team provides call center and office support to active and retired members of client plans, coordinating communications between members and the assigned Plan Administrator. The team processes all member benefits.

Information Technology Group – This team securely maintains all enterprise level hardware and software environments; manages office, network, and internet communications; provides system programming and development; and provides organization and client IT Support.

Office Administration and Support – This team provides reception and clerical support to staff.

Standard Operating Controls

Management sends guidance to employees regarding expected levels of integrity, ethical behavior, and competence. Such practices relate to hiring, orientation, training, evaluation, counseling, promotion, compensation, and remedial actions.

Resource Centers has hiring practices that are designed to help ensure that new employees are qualified for their job responsibilities. All applicants pass through an interview process that assesses their qualifications related to the expected responsibility level of the individual. Resource Centers conducts pre-employment reference checks from information provided on the employment application. Additionally, HR conducts background investigations relating to past employment history, credit history, and criminal activity.

Resource Centers invests significant resources in employee development by providing on-the-job training and other learning opportunities. New employees participate in an orientation program that acquaints them with the

Company's organization, its affiliated companies, functions, values, products, and selected policies. Thereafter, development activities include providing more challenging assignments, job rotation, training programs, seminars, and continuing education programs. Additionally, employees are provided with measurable objectives and are subject to periodic performance reviews to help ensure competence.

Audit

Resource Centers Management performs periodic audits of procedures and holds scheduled compliance meetings with staff to review current and new procedures.

Risk Assessment

Resource Centers has a cross functional risk assessment process that utilizes management, as well as staff, to identify risks that could affect Resource Centers' ability to meet its contractual obligations. Risk assessment efforts include analyses of threats, probabilities of occurrence, potential business impacts, and associated mitigation plans. Risk mitigation strategies include prevention and elimination through the implementation of internal controls and transference through commercial general and umbrella policies.

Team leaders are required to identify significant risks related to their areas of responsibility and implement measures to mitigate those risks. The Partners, which includes the Managing Partner, Chief Operating Officer, and the IT Manager, meet regularly to identify any risks and develop corrective steps to minimize the impact of these risks. The Company employs numerous methods to assess and manage risk, including policies, procedures, team structure, recurring meetings, and automated error detection controls. The Company strives to identify and prevent risks at an early stage through policy and procedure adherence in addition to mitigating relevant risks as discovered either through team structure, meetings, or notifications.

The Company maintains security policies and communicates them to staff to ensure that individuals utilizing Company resources understand their responsibility in reducing the risk of compromise and exercise appropriate security measures to protect systems and data.

Monitoring

The Company regularly monitors the network for capacity, performance, and hardware failure. Overall database health and capacity planning are monitored daily to ensure the system will meet the needs of the Company and its clients. IT monitors security access violations, including server logs and reports.

Monitoring policies and procedures are utilized for addressing issues relating to outages of critical services or other issues needing immediate action. These procedures vary based on the defined severity level of the problem. Company administrators use several monitoring tools to identify and provide alerts to the following conditions:

- A system has exceeded a predefined performance or load threshold.
- A system has suffered an error condition.
- A system has detected a hardware element that is expected to fail in the near future.
- A system is no longer in communication with the monitoring infrastructure.
- A system has entered a condition previously specified by Company administrators as operating outside of a threshold.

Management monitors internal controls as part of normal business operations. The Company uses software to track user and customer requests from initiation until completion. Resource Centers uses a series of management reports and processes to monitor the results of the various business processes. The Management Team regularly reviews the reports and logs, records, and resolves all exceptions to normal processing activities.

Information and Communication

Information Systems

Physical Access

Main Office

Resource Centers' headquarters is located in a multi-tenant professional building residing in Palm Beach Gardens, Florida. Access to the facility is restricted after normal business hours. Only authorized individuals may access the facility after hours via keypad entry.

Access to Resource Centers' suite is through a single entry point that remains locked at all times. Authorized personnel may enter the main entrance by an electronic access control system utilizing electronic keys. Visitors may enter by appointment only. Once allowed access through the main entry, visitors are greeted by a receptionist stationed in the front lobby area. All visitors are escorted by Company personnel throughout their visit with Resource Centers.

Fire Detection and Suppression

Detection sensors are installed in the ceiling of the facility areas. Fire detection equipment is monitored remotely 24x7x365. Suppression devices include handheld extinguishers and a fixed sprinkler system. Fire detection and suppression features include:

- Smoke sensors
- Heat sensors
- Remote 24x7x365 monitoring
- Handheld fire extinguishers
- Fixed sprinkler system

Logical Access

Access to resources and data is granted to individuals based on their job responsibilities. New user accounts are established only upon receipt of properly authorized requests. The security administrator is responsible for ensuring adherence to the security policy that addresses logical access control procedures.

Unique user IDs and passwords are assigned to each user. The Company's security policy establishes password rules that require a minimum of alphanumeric characters with password complexity requirements. Passwords are systematically required to be changed every 42 days. The security administrator sets the user's initial password. The user is required to change the password at first logon.

IT or data owners remove individual access capabilities immediately upon notification of termination of employment, change of responsibilities, or termination of a contract with a client that uses the system. IT and data owners periodically review system security access levels to ensure individual access rights are appropriate based on job information.

User accounts and access rights are managed on the domain controllers employing the Internet-standard Kerberos network authentication protocol to authenticate both the client and the network, and to protect against the possibility of unauthorized users impersonating a server to enter the network.

Database software maintains their respective client databases. The databases are only accessible through the software application and are protected from unauthorized access. No direct network access is granted to this software or the servers that it runs on to anyone other than those granted by IT management.

Network Perimeter Security

The following are complementary types of network security perimeter devices used by the Company on its network to defend Internet-accessible systems:

- Router
- Firewall
- Demilitarized Zone (DMZ)
- Network Address Translation (NAT)
- Virtual Private Network (VPN)

Router

Routers are essential components of the network and control much of the Company's communications. The devices are utilized to divide the network into segments and control traffic flow from one segment to another. Segmenting the network in this manner adds additional levels of security and performance due to the application of traffic flow rules configured on each of the devices. The routers are located in secure, locked rooms to prevent tampering. Logical access to the devices is protected by unique user names and passwords, and can only be utilized by authorized personnel. Additionally, the Company utilizes network monitoring tools to proactively monitor its network for outages.

Firewall

The Company incorporates a firewall at the perimeter of its network to protect against threats from the Internet. The firewall protects the Company's local area network (LAN) from the wide area network (WAN) environment.
The firewall device provides user and application policy enforcement, multi-vector attack protection, and secure connectivity services through a wide range of security and networking services in a unified threat management platform including:

- Application-aware firewall services
- Site-to-site and remote access Internet Protocol Security (IPSec) VPN connectivity
- Intelligent networking services
- Flexible management solutions

De-Militarized Zone (DMZ)

Network computers exposed to the Internet can subject the entire network to hacker attacks. This can lead to compromised data, viruses, and other types of malicious acts that could damage the Company's credibility and operations.

A DMZ has been established to isolate the Company's computers from the Internet. A DMZ is a small network of computers exposed to the external world (Internet). Identifiable security incidents occurring on the DMZ are evaluated, and steps are taken to mitigate those issues and further reduce the risk of breaches of the DMZ.

Network Address Translation (NAT)

The Company uses the technique of NAT on the main Internet router to provide hidden Internet addresses to internal Company computers. This effectively mitigates the possibility of external sources finding the addresses of internal Company computers.

NAT allows computers on a private network to access the Internet through an intermediary called the Network Address Translator. The NAT examines all packets destined for the Internet, removes the private Internet protocol (IP) address from the IP header, substitutes the address of the NAT public interface, and forwards it to the destination. When the resource at the destination IP address responds to the request, the NAT receives it, checks its internal table to see which client the packet belongs to, and forwards it to the proper client.

Virtual Private Network (VPN)

A VPN provides secure, encrypted communication between a network and a remote host or other remote networks over the public Internet. VPNs allow the establishment of an encrypted tunnel that protects the flow of network traffic from eavesdroppers.

A VPN is a private encrypted network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real world connection such as a leased line, a VPN uses virtual connections routed through the Internet from the private network to the remote site or employee.

VPN allows remote users to access the Company's internal network. Users authenticate with the VPN concentrator and then authenticate with the Windows domain to gain access to network resources. Three levels of access rights are implemented based on the type of users accessing the network. Strong VPN authentication and encryption protocols are in use.

Computer Operations

Patch Deployment

The Company takes a proactive approach to patch management. Company administrators regularly monitor various Web sites, message boards, and mailing lists where advanced notification of bug and related patches is often disclosed prior to a public announcement by the vendor. This allows the Company to plan ahead for upcoming patches.

Company administrators consider each patch carefully and independently to determine if it is necessary to deploy it within the production environment. In many cases, the vulnerability addressed by the patch has been mitigated through any number of other countermeasures already in place such as firewalls, the intrusion prevention system, or an aspect of their hardening process. In these cases, patches may be deferred until a future service pack is made available. If Company administrators decide that the patch is necessary and should be deployed, the patch is tested. Once the patch has been thoroughly tested, it is approved for deployment in the production environment.

Data Backup and Restore

Backup

Resource Centers has implemented various backup methods as part of its production operations. The Company has a multi-layered strategy for protecting critical data files to meet business requirements. This strategy includes using hard disk files backed up to external hard drive technology, then to an offsite location using a secured Internet session. Database backup files are created utilizing database backup utilities and then transferred to external drive.

Using an automated process, backup jobs are run using a backup utility whereby the target files are identified in predefined backup jobs. The backup system is monitored continuously by the IT department. Resource Centers also utilizes offline backups that are stored in a safety deposit box which are updated on a monthly basis.

Restore

Restore testing is performed through the course of normal operations and as part of periodic testing. It involves restoring files from external hard drives or may be retrieved from the offsite storage vendor.

Database Security

The production database utilizes security features that encrypt the database at the table and field level to mask Personally Identifiable Information (PII). Access to view masked information is restricted to authorized individuals only.

Description of Operational Controls

Resource Centers has developed and maintained an internal application to process client benefit transactions. The Company also developed a Web-based interface for secured connections via the Internet. The software is not installed in any client environments, nor do clients directly interface with back office development efforts.

The Company has developed roles to achieve their operational controls as follows:

- *The Plan Administrator* serves as a client relationship manager to oversee the daily tasks required to operate the plan and serve as a liaison to the Board and members.
- *The Payment Manager* has primary responsibility to issue payments of benefits and invoices for plans and members.
- *The Accounting Analyst* separately reconciles accounts and transactions, posting activity monthly to the general ledger for each plan.
- *The Accounting Manager* provides management oversight and review for preparation and maintenance of interim plan financial statements.
- *The Data Manager* maintains internal databases used for benefit calculations and reporting.
- *The IT Director* manages the operation of all hardware and software systems used for plan administration.
- *Management* directs internal operations and staff.
- *The Actuary* is the actuarial firm engaged by the Board.
- *The City* is the plan sponsor.
- *The Board* is the local entity established to administer the plan with the authority to delegate operations.

New Participant Plan Enrollment/Client Administration

Management reviews, approves, and executes an Agreement with the Board. Management then issues a detailed transition plan to communicate the tasks to complete the initial client intake. The Plan Administrator updates the Board and Service Provider contact information. Staff then inventory physical Plan records and establish files for Plan records and archive records as appropriate. The Plan Administrator creates a reference archive for Plan records transmitted electronically. The Board provides updated signature authorizations for the Plan Administrator.

The Plan Administrator creates a Plan Web site to provide access to Plan documents and facilitates communication with Plan members. The Board then reviews the template for the Web site.

The Accounting Analyst establishes the chart of accounts and reconciles the trial balance to the reports for the prior period. The Accounting Manager reviews the posting of transactional activity to the general ledger and oversees the production of the interim Plan financial statements.

Management creates an internal written procedure to summarize the Plan provisions based on the local Ordinance, the Summary Plan Description, and the annual valuation. The Board reviews the written procedure.

The Data Manager issues a detail request for historical and current member records to the City.

The Programmer establishes systems to manage the database for the Plan and calculate benefits based on the internal written procedure.

Documents include: a signed Agreement; a transition plan; physical and electronic Plan records; contact information for the Board and Service Providers; signature authorizations; a trial balance and interim financial statements; and a written internal procedure to establish systems.

Pension Benefits Payments

The City provides the necessary data to determine and pay benefits, reported bi-weekly for active members of the plan. The member files an application with the plan for benefits. The Plan Administrator performs benefit calculations at retirement or eligibility. Final calculations require a second internal review before going to the Actuary for certification. The member of the Plan receives a copy of all information used to determine benefits payable under the plan. The Actuary reviews and certifies pension benefit calculations.

The Plan Administrator transmits the instructions for benefit payments to the Payment Manager. The Payment Manager receives and reviews the instructions before paying benefits and distributions due to members of the Plan. The Payment Manager and staff must separately authorize the issuance of any benefit checks or payment batches.

Pension payments are tracked via a payment schedule. The previous monthly payment schedule is compared to the current payment schedule to verify the payment is correct. Any nonconformity is researched and resolved prior to check run. Distributions are processed through the banking institution and are documented in the pension benefit system via a system ready batch file supplied directly to the bank for processing.

Once the check run is approved by the Payment Manager, Magnetic Ink Character Recognition (MICR) toner is installed on the printer and blank check stock is inserted into the proper tray. Client authorized signatures are maintained and systematically digitized on the check signature line. Quality control checks are performed throughout the check run process to ensure the proper check numbers are used and that they are in the proper sequence.

The Accounting Analyst reconciles and records the activity, posting the entries to the general ledger monthly. The Accounting Manager reviews the posting of transactional activity to the general ledger and oversees the production of the interim Plan financial statements. The Board reviews and approves the payment of all benefits from the plan.

The detailed general ledger records the benefit payments to the members of the Plan. The interim monthly financial statements provide a report of this activity to the Board.

Plan Liabilities

The Data Manager tests the member data each year to record all member status changes during the period. The Data Administrator generates reports used for reporting and reconciling the fiscal data. The Accounting Analyst posts all fiscal adjustments and accruals to finalize the fiscal report of Plan assets. The Plan Administrator reports the Plan

assets and the member data each year to the Actuary. The Actuary reconciles the data reports with the Plan Administrator.

The Actuary uses the reports of member data and Plan assets to value and report the liabilities of the plan. The Actuary determines the funding requirements based on the liabilities. The reports generated by the Data Administrator, the Plan Administrator, and the Payment Manager, along with the report of Plan assets detailed in the financial statements, provide the data required by the Actuary to value the liabilities. The reports also form the basis for individual Plan audits and Annual Reports for public safety plans to the Division of Retirement. The annual actuarial valuation reports the liabilities of the Plan.

Invoice Payments

The Plan Administrator reviews invoices for compliance with the agreements on behalf of the Board. The Plan Administrator approves items for payment by the Payment Manager. The Payment Manager and staff pay invoices and other obligations of the plan. The payments post to the general ledger. The Payment Manager and staff are required to separately authorize the issuance of any checks for accounts payable. The Accounting Analyst separately reconciles the accounts monthly and records the activity to the general ledger. The Accounting Manager reviews the posting of transactional activity to the general ledger and oversees the production of the interim Plan financial statements.

The Board reviews and approves the payment of all Plan expenses. The Plan Administrator maintains copies of invoices and authorization for payments. The Board executes a written approval for all Plan expenses. The detailed general ledger records the payments for expenses or other Plan obligations. The interim monthly financial statements provide a report of this activity to the Board.

Automated Clearing House (ACH) Payments

Clients who opt for ACH payment are configured in the application and systematically queued for payment when scheduled payments are ready. There is a dual approval that is required to initiate the ACH process. Once the ACH request is sent to the financial institution, the bank systematically responds with acknowledgement that the file has been received.

Client Reporting and Reconciliation

Employer Contributions

The Actuary determines the required employer contributions based on the liabilities identified in the annual valuation. The Accounting Analyst reconciles and records the amounts deposited to the Plan by the City, posting the entries to the general ledger monthly. The Accounting Manager reviews the posting of transactional activity to the general ledger and oversees the production of the interim Plan financial statements. The actuarial valuation identifies the required contributions annually. The statements for the local checking account or the Plan Receipt & Disbursement Account reflect the dates and amounts for deposits of employer contributions. The detailed general ledger records all of the monthly transactions for the Plan. The interim monthly financial statements provide a report of this activity to the Board.

State Contributions (Police and Fire Plans Only)

The Division of Retirement reports the amount of premium tax receipts available for distribution each year and approves the disbursement of such receipts to the plan. The Comptroller disburses the funds to the City, which transfers the funds in turn to the Plan within three business days of receipt. The Accounting Analyst reconciles and records the amounts deposited to the Plan by the City, posting the entries to the general ledger monthly. The

Accounting Manager reviews the posting of transactional activity to the general ledger and oversees the production of the interim Plan financial statements. The Division of Retirement authorizes the distribution of funds on approval of the Annual Report. The Division reports the amounts distributed to each qualifying Plan in Florida. The detailed general ledger records the premium tax deposits to the Plan. The interim monthly financial statements provide a report of this activity to the Board.

Member Contributions

The City administers the payroll for active members of the plan. The City reports member contributions bi-weekly in two data files, one containing a member record and the other containing cumulative payroll and contribution data for the fiscal year. The Data Manager reviews the data files and appends the updates to the database maintained by the administrator. The Data Manager also checks the data files for internal coherence: contribution totals in the member record file must match the contribution detail in the payroll file for each member. The Programmer has separate responsibility for the coding and maintenance of the data and calculation systems according to the direction provided by Management. The Data Manager matches the member contributions totals in the data files to the deposits by the City.

The Accounting Analyst reconciles and records the amounts deposited to the Plan by the City, posting the entries to the general ledger monthly. The Accounting Manager reviews the posting of transactional activity to the general ledger and oversees the production of the interim Plan financial statements. The data files become the basis for fiscal reports and benefit calculations. The statements for the local checking account or the Plan Receipt & Disbursement Account reflect the dates and amounts for deposits of member contributions. Fiscal reports total pension payroll and contributions for active members. The detailed general ledger records the deposits of member contributions to the Plan. The interim monthly financial statements provide a report of this activity to the Board.

Reporting and Reconciling

Monthly reports can be issued with systematically masked PII to protect client identity. Participants and plan administrators may also access account activity through a secured member area on the Resource Center portal. Staff receive and process incoming and outgoing mail each day related to the receipt or disbursement of funds. Staff copy and log all receipts before depositing amounts automatically. The Accounting Analyst reconciles and records all receipts and deposits to the Plan, posting the entries to the general ledger monthly. The Accounting Analyst also reconciles and records any receipt of funds by wire. The Accounting Manager reviews the posting of transactional activity to the general ledger and oversees the production of the interim Plan financial statements. Receipts other than incoming wires are logged and copied. The local checking account statement reflects the receipt of any incoming wires. The detailed general ledger records all receipts and deposits to the Plan. The interim monthly financial statements provide a report of this activity to the Board.

The Accounting Analyst reconciles accounts, transactions, and reports for the Plan, posting activity to the general ledger monthly. The Accounting Analyst uses monthly consolidated trade date reports to review, reconcile, and record investment activity. The Accounting Manager reviews the posting of transactional activity to the general ledger and oversees the production of the interim Plan financial statements. The auditor reviews and tests the interim Plan financial statements to issue an opinion letter. The Board receives and files the interim monthly financial statements. The Board approves the audited financial statement. The general ledger provides a detailed record of all financial transactions, asset transfers, and changes in asset values.

The interim monthly financial statements provide a summary report conforming to applicable GAAP and GASB standards for the detailed general ledger. The Plan Auditor provides an opinion letter and adjustments to the trial balance following the close of each fiscal period.

Asset Transfers

The Plan Administrator provides instructions to initiate all transfers of assets between managers or accounts held by the Plan. The Plan Administrator has no discretionary authority and functions only within the explicit direction given by the Board. Management, the Board, or the City independently verifies all transfers of assets, including movements of cash between the local checking account and the custodial accounts. The Plan Administrator provides written instruction to initiate transfers of assets. The local checking account statements and the custodial statements provide documentation for asset transfers.

Segregation of Duties

Proper segregation of duties forms an integral part of the internal controls designed to ensure the integrity of the processing and reporting of client transactions. A designated plan administrator authorizes client payments, executed by a separate payment group. Additional staff reconcile statements monthly and post transactions to the client financials. The clients also review and approve all transactions.

Management Oversight

Resource Centers retains a qualified accounting firm to oversee and review the preparation of client financial statements. The accountant provides additional management oversight, third party review of reporting processes and controls, and implementation of accounting standards for client reporting. The clients review monthly reports and approve all transactions.

Change Management

The IT Manager maintains an application development environment separate from production. The Programmer creates and updates applications based on written instruction by the Plan Administrator and approval of Management. The Plan Administrator tests applications and updates provided by the Programmer. Management approves the promotion of applications from development to production. Management maintains an internal application development log to document the process.

Assessing Risk

The Company adheres to a documented information standard and takes a proactive stance in assessing areas of risk. External penetration testing is performed on a predefined basis, as well as real time monitoring of critical systems. Active monitoring for user access to the corporate network and subnetworks is in place to detect and correct any deviations in network traffic and application access.

User Control Considerations

The Company's applications are designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report.

This section describes additional controls that should be in operation at user organizations to complement the controls at the Company. User auditors should consider whether or not the following controls are implemented at user organizations:

- Controls are in place for user organizations to ensure compliance with contractual requirements.
- Controls are in place to ensure that user organizations adopt strong operating system and application password management procedures, including using passwords that cannot be easily compromised and are required to change on a regular basis.
- Controls are in place to provide reasonable assurance of the compatibility of software not provided by Resource Centers
- Controls to provide reasonable assurance that the client has procedures in place for developing, maintaining, and testing their own business continuity plans (BCP).
- Controls to provide reasonable assurance that benefits payment processing occurs in a timely and accurate manner.
- Controls to provide reasonable assurance of the completeness and accuracy of the transmission and receipt of information provided to and received by Resource Centers.
- Controls to provide reasonable assurance incoming payments are received, processed, and posted in a timely and accurate manner.
- Controls to provide reasonable assurance ACH transactions are scheduled, posted, and authorized in a timely and accurate manner.
- Controls for approving the telecommunications infrastructure between itself and Resource Centers.
- Controls are in place to provide reasonable assurance that only authorized users provide transactions to Resource Centers.
- Controls to provide reasonable assurance that reconciliations are completed in a timely and accurate manner.

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Processing of transactions for clients by Resource Centers covers only a portion of the overall internal control structure of each client. Resource Centers' products and services were not designed to be the only control component in the internal control environment. Additional control procedures require implementation at the client level. It is not feasible for all of the control objectives relating to the processing of transactions to be fully achieved by Resource Centers. Therefore, each client's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

III. Information Provided by Ascend Audit & Advisory

Control Objectives, Related Controls, and Tests of Operating Effectiveness

Control Objective 1 – Organization and Administration

CO1 – Controls provide reasonable assurance that Management provides oversight, segregation of duties, and guides consistent implementation of security practices.

C1.0	Controls Specified by Resource Centers	Testing Performed by Ascend Audit & Advisory	Results of Tests
C1.1	Resource Centers has the following corporate policies, reviewed annually and updated as necessary, that guide personnel on procedures within the organization: • Employee Handbook • IT Security Policy • Acceptable Use Policy • Code of Conduct • Disaster Recovery Procedures	Inspected the following corporate policies to determine they were reviewed annually, updated as necessary, and provided guidance to personnel on procedures: • Employee Handbook • IT Security Policy • Acceptable Use Policy • Code of Conduct • Disaster Recovery Procedures	No exceptions noted.
C1.2	An organizational chart, reviewed annually and updated as necessary, is in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel.	Inspected the most current organizational chart to determine: it was reviewed annually; updated as necessary; and communicated key areas of authority, responsibility, and appropriate lines of reporting to personnel.	No exceptions noted.
C1.3	Resource Centers is segregated into separate and distinct functional areas for the purposes of the management of customer information, the processing of the information, and to ensure adequate segregation of duties.	Inspected the most current organizational chart and conducted corroborative inquiry of Management to determine Resource Centers was segregated into separate, logical, and distinct functional areas and that a reasonable segregation of duties existed.	No exceptions noted.

Control Objective 1 – Organization and Administration (Continued)

CO1 – Controls provide reasonable assurance that Management provides oversight and segregation of duties and guides consistent implementation of security practices.

C1.0	Controls Specified by Resource Centers	Testing Performed by Ascend Audit & Advisory	Results of Tests
C1.4	Resource Centers has documented job descriptions that describe the roles and responsibilities of the positions.	Inspected a sample of job descriptions to determine Resource Centers had documented job descriptions that described the roles and responsibilities of the positions.	No exceptions noted.
C1.5	New employees must sign statements confirming acknowledgement of the following: • Employee Handbook • Ethics Agreement • Confidentiality Agreement	For the population of new hires, inspected signed employee acknowledgement forms to determine new employees were required to and signed statements confirming acknowledgement of the following: • Employee Handbook • Ethics Agreement • Confidentiality Agreement	No exceptions noted.
C1.6	On a monthly basis, Management meets to discuss the operations of the business, personnel issues, and strategic plans and financials, as needed.	For the selection of months, inspected monthly meeting minutes to determine Management met to discuss operations, personnel issues, and strategic initiatives on a monthly basis.	No exceptions noted.
C1.7	The Company maintains insurance policies to guard against potential losses due to the following: • General liability • Fiduciary liability • Workers compensation • Crime • Cyber Crime	Inspected the most current insurance declarations to determine the Company maintained insurance policies to guard against potential losses due to the following: • General liability • Fiduciary liability • Workers compensation • Crime • Cyber Crime	No exceptions noted.

Control Objective 2 – Information Security: Physical and Logical Access

CO2 – Controls provide reasonable assurance that physical and logical access to the facility, server room, programs, data, and computer resources is restricted to authorized and appropriate users, and such users are restricted to performing authorized and appropriate actions.

C2.0	Controls Specified by Resource Centers	Testing Performed by Ascend Audit & Advisory	Results of Tests
C2.1	Access to Resource Centers' suite is secured and locked at all times. Authorized personnel may enter by a physical key lock or via keypad entry.	Observed via walkthrough procedures and inspected the office key inventory report to determine access to the Resource Centers suite was secured at all times and only authorized personnel could enter via physical key lock or keypad entry.	No exceptions noted.
C2.2	Access to physical servers and networking equipment is restricted to authorized personnel only.	Observed via walkthrough procedures and recorded digital evidence to determine access to physical servers and networking equipment was restricted to authorized individuals only.	No exceptions noted.
C2.3	All users having access to network resources belong to Active Directory (AD) security groups.	Inspected a screenshot of the Active Directory security groups and associated memberships and conducted corroborative inquiry of IT Management to determine all users with access to the network belonged to AD security groups.	No exceptions noted.
C2.4	A complex password policy is in effect for all authorized users in the corporate network.	Inspected a screenshot of the Active Directory, application, and database password policies to determine a complex password policy was in effect for all authorized users of the corporate network, application, and database.	No exceptions noted.
C2.5	Multi-Factor Authentication (MFA) is required for access to applications within the organization.	Inspected a screenshot of the MFA settings for access to a sample of production applications to determine dual access verification was required.	No exceptions noted.

Control Objective 2 – Information Security: Physical and Logical Access (Continued)

CO2 – Controls provide reasonable assurance that physical and logical access to the facility, server room, programs, data, and computer resources is restricted to authorized and appropriate users, and such users are restricted to performing authorized and appropriate actions.

C2.0	Controls Specified by Resource Centers	Testing Performed by Ascend Audit & Advisory	Results of Tests
C2.6	Administrative access to the Corporate Domain Controller is restricted to authorized personnel only.	Inspected a screenshot of the Local and Enterprise Domain Administrators security group and its membership to determine administrative access to the Corporate Domain Controller was restricted to authorized personnel only.	No exceptions noted.
C2.7	As a component of the employee termination process, a termination notification is sent to Management; system and facility access is revoked; and confirmation of access revocation is communicated.	For the population of terminated users, inspected termination notifications and screenshots of logical access accounts disabled to determine: termination notifications were sent to Management; system and facility access was revoked; and confirmation of access revocation was communicated.	No exceptions noted.
C2.8	Network security event logging is configured to log specific events on the network domain.	Inspected screenshots of the operation system event viewer to determine network security event logging was configured and specific events on the network domain were logged.	No exceptions noted.

Control Objective 3 – Environmental Security

CO3 - Controls provide reasonable assurance that access to secured environments and management of system environments are secured, monitored, and managed.

C3.0	Controls Specified by Resource Centers	Testing Performed by Ascend Audit & Advisory	Results of Tests
C3.1	Fire detection and monitoring are in place to ensure the availability of client data.	Inspected digital evidence of fire and suppression system to determine they were in place during the period under review.	No exceptions noted.
C3.2	Cooling systems are monitored to ensure computing systems availability and temperatures in the server room are regulated.	Inspected the most current monitoring report to determine that temperatures in the server room were regulated and monitored.	No exceptions noted.

Control Objective 4 – Risk Management

CO4 – Controls provide reasonable assurance that risk assessments and internal audit functions are operational and conducted in a timely and accurate manner.

C4.0	Controls Specified by Resource Centers	Testing Performed by Ascend Audit & Advisory	Results of Tests
C4.1	A formal risk assessment is in place and reviewed by Management on an annual basis.	Inspected the most current risk assessment to determine a formal risk assessment was in place and reviewed by Management at least once during the past twelve (12) months.	No exceptions noted.
C4.2	Identified risks are rated using a risk evaluation process and ratings are reviewed by Management.	Inspected the most current risk assessment to determine identified risks were rated using a risk evaluation process and ratings were reviewed by Management.	No exceptions noted.
C4.3	Resource Centers risk identification and assessment process includes identifying and maintaining informational assets with respect to ongoing risk mitigation.	Inspected the most current IT asset inventory registry and risk assessment to determine the Company identified and assessed informational assets with respect to risk mitigation.	No exceptions noted.
C4.4	Web facing systems are tested continuously for known vulnerabilities by a third party application.	Inspected the third party application interface and a sample of log results and email notifications to determine that Web facing systems underwent vulnerability testing during the period under review.	No exceptions noted.

Control Objective 5 – Data Backup and Recovery

CO5 – Controls provide reasonable assurance that data is backed up regularly and is available for restoration in the event of processing errors or unexpected processing interruptions.

C5.0	Controls Specified by Resource Centers	Testing Performed by Ascend Audit & Advisory	Results of Tests
C5.1	Automated backup systems are utilized to perform scheduled system backups of data.	Inspected a screenshot of the backup software management interface to determine an automated backup system was utilized to perform scheduled system backups.	No exceptions noted.
C5.2	Backup jobs are monitored, and notification alerts are sent in the event of backup failure.	Inspected screenshots of system generated backup notifications to determine backup jobs were monitored and notification alerts were sent in the event of backup failure.	No exceptions noted.
C5.3	Data restores are performed as a part of normal business processes and as testing for disaster recovery planning.	Inspected a sample of restore reports to determine data restores were performed.	No exceptions noted.
C5.4	Back up jobs are encrypted to safeguard data during transfer and at rest.	Inspected the backup encryption settings to determine backup procedures included data encryption and time of backup for backup data transfer and at rest.	No exceptions noted.
C5.5	Administrative access to create, modify, and delete backup configurations is restricted to authorized personnel only.	Inspected the administrative user account to determine access to create, modify, and delete backup configurations was restricted to authorized personnel only.	No exceptions noted.

Control Objective 6 – Computer Operations

CO6 – Controls provide reasonable assurance that systems are maintained in a manner that helps ensure system availability and secure against unauthorized access to the network.

C6.0	Controls Specified by Resource Centers	Testing Performed by Ascend Audit & Advisory	Results of Tests
C6.1	A monitoring application is utilized to monitor network devices and critical systems continuously and sends email alert notifications to the IT Manager when predefined thresholds are exceeded.	Inspected screenshots of the monitoring application management console, email notification settings, a sample of alert notifications, and threshold configurations to determine a monitoring application was utilized to monitor the network continuously and sent alerts to IT personnel when predefined thresholds were exceeded.	No exceptions noted.
C6.2	An external monitoring system is utilized to protect the Company's Web sites from automated and external attacks, with respect to managing and mitigating risk. The system provides daily alerts and weekly reports to system administrators for investigatory purposes.	Inspected the third party cyber security management interface along with a sample of alerts and reports to determine a monitoring system was utilized to protect the Company's Web sites from automated and external attacks; and the system generated daily alerts and weekly reports to system administrators.	No exceptions noted.
C6.3	Anti-virus software scans production servers on a real time basis and is configured to automatically update servers on an ongoing basis.	Inspected screenshots of the anti-virus software interface and conducted corroborative inquiry of IT Management to determine anti-virus software scanned production servers in real time and was configured to automatically update servers on an ongoing basis.	No exceptions noted.
C6.4	A firewall is in place to control network traffic and prevent unauthorized traffic from passing between the internal network and external networks.	Inspected a screenshot of the firewall management console to determine a firewall was in place to control network traffic and prevent unauthorized traffic from passing between the internal network and external networks.	No exceptions noted.
C6.5	Administrative access to the firewall appliance is restricted to authorized users only.	Inspected a screenshot of the administrator IP address range configuration to determine administrative access to the firewall was restricted to authorized users only.	No exceptions noted.

Control Objective 6 – Computer Operations (Continued)

CO6 – Controls provide reasonable assurance that systems are maintained in a manner that helps ensure system availability and secure against unauthorized access to the network.

C6.0	Controls Specified by Resource Centers	Testing Performed by Ascend Audit & Advisory	Results of Tests
C6.6	Administrative sessions for the firewall are configured to timeout after a predefined period of inactivity.	Inspected a screenshot of the firewall session expiration length setting to determine administrative sessions for the firewall were configured to time out after a predefined period of inactivity.	No exceptions noted.
C6.7	Network Address Translation (NAT) services are enabled on the network firewalls. Internal production servers do not have routable IP addresses.	Inspected a screenshot of the network routing table and conducted corroborative inquiry of IT Management to determine NAT services were enabled on the network firewall, and internal production servers did not have routable IP addresses.	No exceptions noted.
C6.8	VPN connections are utilized by authorized staff to establish encrypted communication sessions to the corporate network.	Inspected a screenshot of the remote VPN user access control list to determine VPN connections were utilized by authorized staff to establish encrypted communication sessions to the corporate network.	No exceptions noted.
C6.9	Secure communication tunnels are in place for file transfers requiring encryption to Resource Centers' Web servers through the use of Secure Sockets Layer (SSL) encryption.	Inspected the most current SSL certificate to determine secure communication tunnels were in place for file transfers requiring encryption to the Company's Web servers and utilized SSL encryption.	No exceptions noted.
C6.10	A Secure File Transfer Protocol (SFTP) server is utilized for encrypted file transfers and is monitored and administered by the IT Department.	Inspected the SFTP configuration and conducted corroborative inquiry of IT management to determine a SFTP server was utilized for encrypted file transfers and was monitored and administered by the IT Department.	No exceptions noted.

Control Objective 6 – Computer Operations (Continued)

CO6 – Controls provide reasonable assurance that systems are maintained in a manner that helps ensure system availability and secure against unauthorized access to the network.

C6.0	Controls Specified by Resource Centers	Testing Performed by Ascend Audit & Advisory	Results of Tests
C6.11	An Intrusion Prevention System (IPS) is utilized to monitor the network 24x7x365 for malicious activity and unauthorized access attempts. The IPS is configured to alert administrators when predefined thresholds are exceeded regarding access attempts and malicious code.	Inspected the configuration of the IPS, activity logs, and reports and conducted corroborative inquiry of IT management to determine the IPS was in place, monitored the network continuously, and provided alerts to administrators when predefined thresholds were exceeded regarding access attempts and malicious code.	No exceptions noted.
C6.12	Policies and procedures are in place for patch management on production systems.	Inspected the patch management update history and conducted corroborative inquiry of IT management to determine procedures were in place for patch management on production systems.	No exceptions noted.

Control Objective 7 – Change Management

CO7 – Controls provide reasonable assurance that changes to the application programs and related data management systems are authorized, tested, documented, approved, and implemented to result in complete, accurate, and timely processing and reporting.

C7.0	Controls Specified by Resource Centers	Testing Performed by Ascend Audit & Advisory	Results of Tests
C7.1	A development lifecycle log is maintained to track code builds throughout the development lifecycle and document approvals.	Inspected the application development log and conducted corroborative inquiry of Management to determine a development lifecycle log was maintained to track code builds and document approvals.	No exceptions noted.
C7.2	Changes are documented, tickets are submitted, and changes are tracked through completion.	Inspected the application development log and conducted corroborative inquiry of Management to determine changes were documented and tracked through completion.	No exceptions noted.
C7.3	System changes require approval by Management prior to implementation.	Inspected the application development log and conducted corroborative inquiry of Management to determine system changes required and received approval by Management prior to implementation.	No exceptions noted.
C7.4	Separate source code environments exist for development, testing, and production to prevent making changes that would affect the performance, availability, and integrity of production application code.	Inspected a screenshot of the network topology diagram to determine separate source code environments existed for development, testing, and production.	No exceptions noted.
C7.5	Administrative access to the production environment is restricted to appropriate personnel.	Inspected the secure login interface to the production environment to determine administrative access to production was restricted to authorized personnel.	No exceptions noted.

Control Objective 8 – Pension Benefits Payments

CO8 – Controls provide reasonable assurance that distributed client payments are complete, accurate, and timely.

C8.0	Controls Specified by Resource Centers	Testing Performed by Ascend Audit & Advisory	Results of Tests
C8.1	Upon retirement or eligibility, the member completes an application for pension plan benefits and acknowledges payment options and plan terms.	For the selection of eligible members, inspected signed applications to determine the member completed an application for pension benefits and acknowledged payment options and plan terms.	No exceptions noted.
C8.2	Resource Centers obtains the approved final benefit calculation from the external actuary and obtains the completed application for pension plan benefits from the eligible member prior to disbursement.	For the selection of eligible members, inspected the approved benefit calculations; and for a sample of eligible members observed via walkthrough procedures, the benefit calculations process to determine the Company obtained the final benefit calculation from the external actuary prior to disbursement. For the selection of eligible members, inspected signed applications to determine the Company obtained completed applications for pension plan benefits from eligible members prior to disbursement.	No exceptions noted. No exceptions noted.
C8.3	The Plan Administrator creates the appropriate distribution form based upon the member's benefit election, which is reviewed by a second Plan Administrator prior to disbursement.	For the selection of members, inspected signed and reviewed distribution forms and conducted corroborative inquiry of Management to determine the Plan Administrator created the appropriate distribution based on the member's election; and a second Plan Administrator reviewed prior to disbursement.	No exceptions noted.
C8.4	Prior to disbursement, the previous payment activity report is systematically compared to the current report and checked for nonconformities.	For a sample of eligible members, observed via walkthrough procedures and conducted corroborative inquiry of Management to determine that prior to disbursement the previous payment activity report was compared to the current report and checked for nonconformities.	No exceptions noted.

Control Objective 8 – Pension Benefits Payments (Continued)

CO8 – Controls provide reasonable assurance that distributed client payments are complete, accurate, and timely.

C8.0	Controls Specified by Resource Centers	Testing Performed by Ascend Audit & Advisory	Results of Tests
C8.5	A segregation of duties exists for ACH and tax request and approval prior to processing.	For a sample of clients, inspected bank authorization emails for ACH processing, accompanying batch processing receipts and confirmations, and completed tax payment request forms to determine there was a segregation of duties between requestor and approval personnel prior to ACH and tax processing.	No exceptions noted.

Control Objective 9 – Client Reconciliation and Reporting

CO9 – Controls provide reasonable assurance that procedures are in place to deliver monthly payment reporting in a complete and accurate manner.

C9.0	Controls Specified by Resource Centers	Testing Performed by Ascend Audit & Advisory	Results of Tests
C9.1	Employee contribution data submitted by clients is reconciled to Resource Centers' database. Variances are researched and resolved.	For a sample of clients observed via walkthrough procedures employee contribution reconciliation files and payroll post confirmations to determine employee contribution data submitted by clients was reconciled to the Company's database.	No exceptions noted.

Control Objective 10 – Client Administration

CO10 – Controls provide reasonable assurance that documents reflecting the plan sponsor's intent to do business are properly authorized.

C10.0	Controls Specified by Resource Centers	Testing Performed by Ascend Audit & Advisory	Results of Tests
C10.1	Prior to client implementation, Resource Centers obtains signed agreements and pension summary approval from the Board.	For the population of new clients, inspected signed agreements, pension summary forms, and Board meeting minutes to determine Resource Centers obtained required agreements, plan details, and approvals prior to client implementations.	No exceptions noted.