



A-LIGN



The Retirement  
Systems of Alabama  
Type 2 SSAE 16  
2016



**REPORT ON MANAGEMENT'S DESCRIPTION OF THE RETIREMENT SYSTEMS  
OF ALABAMA'S SYSTEM AND THE SUITABILITY OF THE DESIGN AND  
OPERATING EFFECTIVENESS OF CONTROLS**

**Pursuant to Statement on Standards for Attestation Engagements No. 16  
(SSAE 16) Type 2**

**October 1, 2015 Through September 30, 2016**

# Table of Contents

<b>SECTION 1 INDEPENDENT SERVICE AUDITOR’S REPORT .....</b>	<b>1</b>
<b>SECTION 2 THE RETIREMENT SYSTEMS OF ALABAMA’S ASSERTION .....</b>	<b>4</b>
<b>SECTION 3 DESCRIPTION OF THE SYSTEM PROVIDED BY THE SERVICE ORGANIZATION .....</b>	<b>7</b>
OVERVIEW OF OPERATIONS .....	8
Company Background .....	8
Description of Services Provided .....	8
CONTROL ENVIRONMENT .....	13
Integrity and Ethical Values .....	13
Commitment to Competence .....	14
Board of Directors Participation .....	14
Management’s Philosophy and Operating Style .....	15
Organizational Structure and Assignment of Authority and Responsibility .....	15
Human Resources Policies and Practices .....	15
RISK ASSESSMENT .....	16
CONTROL OBJECTIVE AND RELATED CONTROL ACTIVITIES .....	17
MONITORING .....	18
INFORMATION AND COMMUNICATION SYSTEMS .....	18
Information Systems .....	18
Communication Systems .....	20
COMPLEMENTARY USER ENTITY CONTROLS .....	20
<b>SECTION 4 TESTING OF CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES PROVIDED BY THE SERVICE AUDITOR .....</b>	<b>22</b>
GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR .....	23
PHYSICAL SECURITY .....	24
ENVIRONMENTAL SAFEGUARDS .....	26
COMPUTER OPERATIONS - BACKUP .....	28
COMPUTER OPERATIONS - AVAILABILITY .....	30
DATA COMMUNICATION .....	32
INFORMATION SECURITY .....	34
CHANGE MANAGEMENT .....	37
ENROLLMENT .....	38
CONTRIBUTIONS .....	40
DISTRIBUTIONS .....	42
ERS/TRS/JRF - VALUATION .....	45
INVESTMENT MANAGEMENT .....	51

**SECTION 1**  
**INDEPENDENT SERVICE AUDITOR'S REPORT**

**INDEPENDENT SERVICE AUDITOR'S REPORT ON A DESCRIPTION OF THE RETIREMENT  
SYSTEMS OF ALABAMA'S SYSTEM AND THE SUITABILITY OF THE DESIGN  
AND OPERATING EFFECTIVENESS OF CONTROLS**

To The Retirement Systems of Alabama:

We have examined The Retirement Systems of Alabama's (Teachers' Retirement System of Alabama (TRS), Employees' Retirement System of Alabama (ERS) and Alabama Judicial Retirement Fund (JRF) collectively known as 'RSA' or 'the Company') description of its Pension Administration system at its Montgomery, Alabama location for processing user entities' transactions for the period October 1, 2015 through September 30, 2016, 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 RSA'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 and operating effectiveness of such complementary user entity controls.

RSA uses Bloomberg for financial software tools for analytics, equity trading and data services, Eze Software Group for trade order management services, Omgeo for US based financial markets trade allocation services, State Street Bank as a U.S based international financial services holding company, SunGard to provide accounting and portfolio management solutions, and TradeWeb Markets LLC as a provider of electronic over-the-counter marketplaces ("subservice organizations"). The description in Section 3 includes only the controls and related control objectives of RSA and excludes the control objectives and related controls of the subservice organizations. Our examination did not extend to controls of the subservice organizations.

In Section 2 of this report, RSA has provided an 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. RSA 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.

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 for the period October 1, 2015 through September 30, 2016.

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 in Section 2. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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.

In our opinion, in all material respects, based on the criteria described in RSA's assertion in Section 2 of this report:

- the description fairly presents the system that was designed and implemented for the period October 1, 2015 through September 30, 2016
- 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 for the period October 1, 2015 through September 30, 2016 and user entities applied the complementary user entity controls contemplated in the design of RSA's controls for the period October 1, 2015 through September 30, 2016
- 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, and operated effectively for the period October 1, 2015 through September 30, 2016

The specific controls tested and the nature, timing, and results of those tests are listed in Section 4.

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of RSA, user entities of RSA's system during some or all of the period October 1, 2015 through September 30, 2016, and the independent auditors of such user entities, who 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 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.

A handwritten signature in black ink that reads "A-LIGN". The letter "A" is significantly larger and more stylized than the other letters, which are in a simple, clean font.

October 14, 2016  
Tampa, Florida

**SECTION 2**  
**THE RETIREMENT SYSTEMS OF ALABAMA'S ASSERTION**



## The Retirement Systems of Alabama's Assertion

October 14, 2016

We have prepared the description of The Retirement Systems of Alabama's (Teachers' Retirement System of Alabama (TRS), Employees' Retirement System of Alabama (ERS) and Alabama Judicial Retirement Fund (JRF) collectively known as 'RSA' or 'the Company') Pension Administration System for user entities of the system during some or all of the period October 1, 2015 through September 30, 2016, 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 Pension Administration System made available to user entities of the system during some or all of the period October 1, 2015 through September 30, 2016 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:
    - (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 the service organization's controls.
    - (7) Other aspects of our control environment, risk assessment process, information and communication systems (including 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 the Pension Administration System, while acknowledging that the description is prepared to meet the common needs of broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the Pension Administration 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 for the period October 1, 2015 through September 30, 2016 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 the service organization;
  - 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, including whether manual controls were applied by individuals who have the appropriate competence and authority.



\_\_\_\_\_  
Diane E. Scott, CPA, CGMA  
Chief Financial Officer  
The Retirement Systems of Alabama

**SECTION 3**  
**DESCRIPTION OF THE SYSTEM PROVIDED  
BY THE SERVICE ORGANIZATION**

## OVERVIEW OF OPERATIONS

### Company Background

Retirement Systems of Alabama is the administrator of the pension funds for Teachers' Retirement System (TRS), Employees' Retirement System (ERS) and Judicial Retirement Fund (JRF). RSA Headquarters is located in Montgomery, AL. RSA ranks as one of the largest public pension funds in the United States.

Retirement Systems of Alabama includes three separate pension funds that support the retirement plans of its members that are included in the scope of this report. These funds include the Employees' Retirement System of Alabama, Teachers' Retirement System of Alabama, and the Alabama Judicial Retirement Fund. The Employees' Retirement System was established in 1945 to provide retirement and other benefits to state employees, state police, and on an elective basis to qualified persons of cities, towns, and quasi-public organizations. Since 1939, The Teachers' Retirement System has provided benefits to qualified members employed by state-supported educational institutions, including public employees of K-12 school systems, two-year Community Colleges, four-year higher education institutions, and state education agencies. The Judicial Retirement Fund was established under the provisions of Act 1163 of the Legislature of 1973 to provide benefits to qualified judges and justices. The ERS Board of Control administers and manages the JRF. The JRF, ERS, and TRS are defined benefit plans qualified under Section 401(a) of the Internal Revenue Code. The goal is to provide exceptional member services, including accurate and timely benefit payments to our eligible retirees, beneficiaries and survivors.

### Description of Services Provided

#### *Enrollments*

The Code of Alabama 1975, Title 16, Chapter 25 (TRS), Title 36, 27 (ERS), and Title 12, Chapter 18 (JRF) provides the State laws and regulations for the respective Benefits processes. TRS is governed by the TRS Board of Control. ERS & JRF are both governed by the ERS Board of Control. Procedures for the employer and employee participation have been documented and established by the Code of Alabama 1975.

RSA receives enrollment forms submitted by participating units on behalf of their employees for processing and the establishment of the initial member account. An enrollment form is submitted to RSA through the Office Services Department. The form is scanned into Library Manager where the electronic image is stored. Members of Office Services process new enrollments within Library Manager on a timely basis. Enrollment forms are processed through the workflow system within Work Manager to help ensure the forms are processed completely and in a timely fashion. Incomplete enrollment forms are automatically routed to a queue to be resolved by the ERS, TRS, or JRF Benefits Departments. The information from the form is manually entered into the Library Manager system. This system will detect duplicate enrollments and notify the user. Library Manager requires a secondary review of new enrollment data by an operator of Office Services. The new information is routed to ITS and Member Online Records are updated nightly in batch processing.

An employee in the ERS, TRS, or JRF department manually reviews the enrollment form by checking for completeness and accuracy. This employee has been trained by a supervisor on determining if the eligibility requirements have been met. Access to update new enrollment data within the workbench system is limited to appropriate personnel.

Contributions from participating units are also submitted to RSA through the Revenue Accounting Department. If a contribution is submitted for a new employee who does not have an existing member file (the enrollment form has not been submitted), the member's Library Manager account folder will be automatically created and filed in the corresponding Library Manager agency file without undergoing the enrollment form process. New member enrollment forms are required to be completed as part of the new member enrollment process. Where a new member form is not submitted, the employer must submit necessary new member data as part of the contribution process.

## *Contributions*

The RSA receives contribution remittances from three main sources: TRS Units, Local Units, and the State Comptroller's Office (State Employees, State Police, and Judges).

The Code of Alabama 1975 provides laws and regulations for contributions to the TRS, ERS, and JRF plan. The specific Code Sections for each System are referenced in the Internal Control Documentation of the respective Systems. Also, the Boards of Control for the respective Systems ensure the laws and limitations relating to contributions are followed. Units seeking to join the RSA must submit a request requiring approval from the Board of Control. Contribution requirements and limitations are described in the law and monitored by RSA staff.

Units are assigned a specific Unit Code by the appropriate Benefits section. The Revenue Accounting and ITS Departments are then notified of the new Unit and Unit Code. When contributions are received in the Revenue Accounting Department, they cannot be recorded by the Revenue Accounting Staff unless an accurate Unit Code is entered. Contributions posted must be from an approved unit with a valid contribution code.

Unit Contributions Remittance Report files are uploaded successfully to the Contribution Reporting Application (CRA) website and checks are delivered to Accounting by the RSA mail room. The Revenue Accounting Staff open the mail and verify that the remittance sheet and the check/checks balance. Accounting reviews the clerical accuracy of the contribution forms and the cash receipt amounts are reviewed for completeness and accuracy before funds are posted to member accounts. The control total (remittance amount) is reconciled to the total member contributions amount.

Accounting restrictively endorses contribution checks upon receipt and deposits check receipts daily via Regions Bank's Remote Quick Deposit Program. Accounting controls access to receipts by storing them in a secure cabinet to prevent unauthorized access to cash receipts and to prevent unrecorded cash/check receipts. Checks are deposited into the bank via the Remote Quick Deposit provided by Regions. Bank deposits containing currency are still sent to the bank by a bonded courier service. A copy of the deposit slip is returned from the Bank by the courier the following day and validated by accounting personnel. RSA Revenue Accounting staff will ensure that the funds were correctly posted for the prior days' ERS and TRS receipts. A daily roll-forward from the prior day's ledger balance is performed by the Revenue Accounting department to ensure that the funds were correctly posted for the prior day's JRF receipts.

The RSA Revenue Accounting Department runs a Past Due Contributions Report listing units that have not uploaded and remitted the required monthly contribution to help ensure that members are receiving the appropriate credit for amounts withheld from unit payrolls.

## *Distributions*

There are four types of benefit payrolls: three types of weekly payrolls and one monthly payroll. The three types of weekly payrolls are withdrawal, DROP and supplemental. For weekly payrolls, the final Daily Reconciliation Report for the week is compared to the weekly Payroll report by Accounting Staff, and any discrepancies are investigated. Two individuals with signature authority (Authorized Voucher Signors as documented by RSA) are required to approve the weekly payroll report. The weekly benefit checks are counted by Member Payroll Personnel and the total is compared to the number of checks per the payroll report to ensure completeness.

Monthly payrolls include the monthly retirement and beneficiary payments. After the monthly benefits payroll is run, the File Balance Report is generated and balanced to the corresponding balancing spreadsheet for both the regular retiree monthly payroll and the monthly DROP payroll (through June 2016). Two individuals with signature authority (Authorized Voucher Signors as documented by RSA) approve the monthly benefit payrolls. After retirement payments are finalized, a Payroll Summary is prepared by Member Payroll Personnel and delivered to the retirement plan's management for review.

## Valuations

The Retirement Systems of Alabama (RSA) provides the actuary with census data files to complete the annual actuarial valuations for ERS, TRS, & JRF. The files that are provided to the actuary include ERS, TRS, & JRF actives, retirees, DROP members, & T-Section members. Supplemental schedules containing additional information needed by the actuaries are also sent to the actuary. All actuarial valuation data files sent to the actuaries are encrypted and password protected.

Active files contain participant data on existing active members, inactive members, and active/inactive members who withdrew during the current year. The active files include participant data such as the valuation year, valuation code, unit code, register/account number, social security number, PID number, date of birth, date of death (if applicable), gender, job classification code, account status, employment date, withdrawal date & cause (if applicable), service credit (in months), cumulative current year and prior year member contributions and interest, current and prior year compensation (based on actual contributions), and number of service months earned during fiscal year. The ERS Active file includes records for both ERS & JRF members. Classification codes for JRF actives are obtained each year from the Court System (or other reliable source) and are updated in the valuation files using an update query. The participant data that is contained in the active files is tested for completeness and accuracy.

Testing of the active valuation files includes but is not limited to the following:

- Total count of active and inactive members
- Total count of withdrawn members by type
- Total amount of compensation for active members
- Member contributions per the valuation file
- Makeup/purchased service contributions per the valuation file
- Ending annuity savings fund amount per the valuation file
- Regular withdrawal amounts per the valuation file
- Death withdrawal amounts per the valuation file
- Amounts transferred out for retirement per the valuation file

Valuation data files are compared to the general ledger accounts at fiscal year-end to test the accuracy and completeness.

Retired files contain participant data on retired members and beneficiaries who are receiving retirement benefits, suspended retired members (i.e. DROP members have a suspended status in the retired file while in DROP), & terminated retirees. Retired file participant data includes: retiree SSN, retiree name, gender, date of birth, classification code, valuation code, unit code, account status, termination cause/type (if applicable), retired account number, retirement type, membership date, retirement date, date of death (if applicable), average final compensation, retirement option selection, maximum benefit allowable, monthly benefit including COLAs, fiscal year and cumulative amounts paid to member, total amount of member contributions/interest, and beneficiary information such as beneficiary's SSN, name, gender, date of birth, fiscal year and cumulative amounts paid to beneficiary (if applicable). The ERS Retired file includes records for both ERS & JRF members.

Testing of the retired files includes but is not limited to the following:

- Compare the number of retirees by account status to the prior year
- Compare the number of retirees by retirement type to the prior year
- Compare the retirement benefit amounts per the valuation file to the general ledger

The actuarial valuation files are checked for missing data such as dates of birth, gender, class code, employment date, and service credit to ensure the completeness of the census data. Any missing information that is identified is sent to the ERS/TRS Benefits Divisions to obtain. The Benefits Division will then send the information back to the Accounting Department where an update query is run in Microsoft Access to update the necessary information in the valuation file. The missing information is also placed in the legacy system.

Various analytical review procedures are performed to test the accuracy and completeness of the actuarial valuation files. Additional procedures performed include but are not limited to:

- Compare the calculated death benefit, administrative expense, and term life (TRS only) amounts based on the compensation in valuation file to the general ledger account balances
- Check that employment and withdrawal dates are included throughout the fiscal year and that there are none after fiscal year-end
- Compare count of retirees/beneficiaries receiving benefits per the valuation file to the count maintained by Accounting Payroll
- Check that retirement dates are included throughout the fiscal year and that there are no retirement dates included after fiscal year-end
- Identify unreasonable dates of birth, retirement dates, etc., investigate, and correct if necessary

Deferred Retirement Option Program (DROP) File (applies to TRS and ERS) - The DROP file contains participant data on DROP members such as SSN, account number, DROP entry date, annual salary, contributions & interest, DROP benefits & interest, withdrawals, and forfeitures.

DROP (Deferred Retirement Option Program) file testing includes:

- Selecting a sample from the actuarial valuation files to compare data to the member's fiscal year-end statement from the RSA DROP System to verify the accuracy of the file data
- Valuation file data is compared to the general ledger accounts at fiscal year-end to test the reasonableness of the valuation file data including DROP contributions, benefits, interest distributions, forfeitures, and beginning and ending DROP equity

All actuarial valuation data files are sent to the actuary upon approval by RSA's CFO. Upon completion of the valuations, the actuaries provide RSA with preliminary results including draft actuarial valuation reports for ERS, TRS, and JRF. The draft copies are reviewed by RSA Accounting staff and RSA CFO.

In order to further validate the completeness and accuracy of the active census data, the following are provided to participating units at the end of each plan year (June 30 for TRS and September 30 for ERS and JRF):

- Account Statement Listing - lists all active members and inactive members who have not retired from the respective unit. This list contains the data elements of name, Social Security Number (last four), entry date, date of birth, account balance, contributions life to date, interest life to date, and beneficiary information. Units may use this to report errors in census data to RSA
- Annual Check List - lists all members for which the unit submitted a contribution for the preceding plan year along with their name, Social Security number (last four), amount of contributions, service credit earned and designated membership Tier. TRS units are required to review the report, note any necessary corrections, certify to its correctness and return to TRS Benefits for review and correction. ERS units are encouraged to return a certified copy of the reviewed documents

Finally, annual statements are mailed to all active and inactive members of TRS, ERS, and JRF listing service credit, contributions and interest by year along with total account balance.

### *Investment Management*

The Boards of Control invest and reinvest System funds in accordance with the Prudent Man Rule: “with the care, skill, prudence, and diligence under the circumstances then prevailing that a prudent man acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims.” Other funds currently under the management of the Systems are governed by the Investment Policy Statement within each System’s limitations and/or by other applicable legislated restrictions. Investment policies and procedures are in place to provide guidelines to the RSA employees responsible for executing investment transactions.

The Investment Committee of each System approves that all investments are made within the prescribed investment policy. These Investment Committees, in their approval, are considered to be signing for the respective Board of Control. If any purchase or sale is questioned by a member of the respective Investment Committee as to whether it is within given Board policy, the Board decides and no purchase or sale takes place until all parties are in agreement. Investment transactions are processed after completion in the trade order management system and upon receipt, signed trade tickets are reviewed for adherence to approved criteria and authorization by the CEO and respective Investment Committee Members.

All trades and investment positions are booked to the accounting system. Monthly reconciliations are performed by Investment Accounting to help ensure that general ledger investment account balances are in agreement with the custodian of the funds and that investment activity had been posted to the correct accounts.

### *Significant Events*

RSA has implemented automated and manual procedures to capture and address significant events and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with detailed information that impacts the Pension Administration system. Please see the procedures, monitoring, and risk assessment procedures described in the relevant sections of this report for further details.

### *Functional Areas of Operation*

The RSA staff provides support for the above services in each of the following functional areas:

<b>Department</b>	<b>Description</b>
Information Technology	The Information Technology (“IT”) Staff is responsible for activities associated with developing, maintaining and supporting critical data processing systems. The organizational structure of the Information Technology staff provides segregation of duties between client services, systems programming, application programming, computer operations, physical and logical security access and documentation
Benefits	The Benefits Staff is responsible for day-to-day benefit processing. This includes weekly and monthly retirement benefit processing for members and beneficiaries. Benefits also performs enrollment, account maintenance, and withdrawal processes for active members and units
Investment	The Investment Staff is responsible for investing, executing, and reinvesting System funds. This includes management of trades and investment positions

Department	Description
Accounting	Accounting Staff is responsible for receiving, identifying, posting and depositing all contribution payments received each day in a timely and accurate manner. Accounting is also responsible for member payroll distribution, and valuation production. Monthly reconciliations are performed by Investment Accounting to help ensure that general ledger investment account balances are in agreement with the custodian of the funds and that investment activity had been posted to the correct accounts, Member Payroll processes the monthly and weekly payrolls for retiree benefit payments, withdrawals, and death payments

### **Boundaries of the System**

The scope of this report includes the Pension Administration system performed in the Montgomery, AL facilities for Teachers Retirement System of Alabama, Employees' Retirement System of Alabama and Alabama Judicial Retirement Fund.

### **Subservice Organizations**

RSA uses Bloomberg for financial software tools for analytics, equity trading and data services, Eze Software Group for trade order management services, Omgeo for US based financial markets trade allocation services, State Street Bank as a U.S based international financial services holding company, SunGard to provide accounting and portfolio management solutions, and TradeWeb Markets LLC as a provider of electronic over-the-counter marketplaces ("subservice organizations"). No subservice organizations were included in the scope of this assessment.

### **Significant Changes Since the Last Review Period**

No significant changes have occurred to the services provided to user entities since the organization's last review.

## **CONTROL ENVIRONMENT**

### **Integrity and Ethical Values**

Management conveys integrity and ethical values to all levels of RSA staff to help with performance and monitoring of business functions. RSA is an entity of the State of Alabama and accordingly has several standard behavior requirements including but not limited to Statutes creating each entity. One example from the TRS statute and is similarly stated in the others is as follows: "all of its business shall be transacted, all of its funds invested and all of its cash and securities and other property held in trust for the purpose for which received." RSA is managing assets in trust specifically for the benefit of many. All employees are subject to the Ethics law of the State of Alabama (Section 36-25-1 et.seq., 1975 Code of Alabama) which prohibits any employee from using the position for personal gain. All employees who earn over \$75,000 per year and all full-time non-merit employees must file a Statement of Economic Interests with the State Ethics Commission. RSA has an Investment Manual designed to assist investment staff in matters regarding system procedures, rules, and regulations for investments that addresses issues such as professional conduct, confidentiality, and legal requirements. All personnel are subject to the IT Security Policy Manual as well as the Human Resources policies and procedures. Furthermore, the Examiners of Public Accounts has the authority to perform on a bi-annual basis legal compliance audits of all entities within the RSA.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational policy statements and codes of conduct are documented and communicate entity values and behavioral standards to personnel. The employee policy and procedures manual contains organizational policy statements and codes of conduct to which employees are required to adhere
- Policies and procedures require that employees sign an acknowledgment form indicating that they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook

### **Commitment to Competence**

RSA's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

### **Board of Directors Participation**

Overall, the Board of Directors and associated committees coordinate their meetings and efforts with the personnel in the office of the CEO.

Corporate governance encompasses the internal policies and practices by which the RSA is operated and controlled on behalf of the State and its members. The advantages of sound corporate governance include having strong Boards of Control that are accountable to the State, RSA, and its members. No member of RSA executive staff is a member of either of the governing boards. The boards consist of members of the systems either appointed by the Governor, elected by the membership, or holding the board position because of their primary government position including but not limited to the Governor, State Treasurer, State Superintendent of Education and Finance Director. The duties and responsibilities of the governing boards are outlined in the statutes under which they were created.

The TRS Board is scheduled to meet semi-annually, with special meetings held as the Board's business may require. Per a resolution passed by the ERS Board of Control at its December 2013 meeting, the ERS Board meets quarterly, with special meetings held as the Board's business may require. All Board meetings and any committee meetings are held with public notice filed with the Secretary of State of Alabama in advance of the meeting with agendas and packages of information made available to members in advance of the meeting. Ad hoc committees work with RSA staff to assure that the meetings and actions or recommendations are submitted to the full board for approval or acceptance.

The system of governance followed by the RSA and documented in the enabling legislation for each respective entity is intended to give surety that the Boards will have the necessary power and practices in place to review and evaluate the RSA business operations and to make decisions that are independent of the RSA management.

## Management’s Philosophy and Operating Style

To fully demonstrate the appropriate application of this principle, RSA should display the following attributes: appropriate tone; influence over attitudes toward accounting principles and estimates; and an articulation of its objectives. RSA believes these attributes are more fully described and addressed in other sections of this document and to avoid duplication has provided cross references to the appropriate section, as described in the chart below:

Attribute of the Principle	Addressed in Section
Sets the appropriate tone	Integrity and Ethical Values
Influences attitudes towards accounting	Fraud Risks
Articulates objectives	Risk Assessment

## Organizational Structure and Assignment of Authority and Responsibility

The Company’s organizational structure provides the framework within which activities for achieving objectives are planned, executed, controlled and monitored. The organizational structure described below details the departments of the service organization that provide Customer Services for its clients. The structure provides for an adequate segregation of duties as well as clearly defined areas of responsibility.

## Human Resources Policies and Practices

RSA’s success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel, from the clerical staff to the management team who ensures the service organization is operating efficiently.

RSA Human Resources (HR) carries out the policies and procedures mandated by the State Personnel department. HR policy development for RSA is performed by the HR group that is operating at the corporate level. This group reviews, amends, or processes new policies to include workplace behavior policies, workplace compliance policies, and staffing policies, as determined necessary.

The content of these policies and additional policy requirements are reviewed on an as needed basis. HR monitors various external and internal policy drivers to proactively determine if changes need to be made. In the event policies require changes or creation, the HR group drafts the policy and reviews it with senior management. All policy changes must be approved by the CEO, Deputy Director or General Counsel.

Approved HR policies are documented and communicated to employees through various channels, including placement on the RSA intranet and verbally through senior management. RSA employees are encouraged to review policies on a regular basis through the appropriate channels. Additionally, employees must agree to adhere to RSA and HR policies.

Policy violations can be reported in a variety of methods including but not limited to their immediate or senior supervisor, division head, and direct contact with HR. Policy violations normally result in disciplinary action ranging from oral reprimand to dismissal in accordance with RSA policies and within guidelines established under statute by the State Personnel Department.

RSA complies with State Personnel procedures in hiring of administrative staff covered by the State Merit system. For specific professional level personnel RSA employs in unclassified positions, RSA establishes minimum criteria and screens applicants through interviews and reference checks.

When it is determined that a position needs to be filled, the RSA manager informs HR of the appropriate information related to the position.

The HR group monitors all applicants and requires steps in the hiring process to be completed by both the hiring manager as well as others as deemed necessary prior to a position being filled. At the beginning of the recruitment process, the hiring manager works with staffing to define skills and position requirements. If the position being filled is a current position, the existing job description is typically used. In the event the position does not exist or it is unique or has unique functions, the hiring manager works with HR to set the job description and pay scale. Once the position has been defined, it must be approved by the Deputy Director prior to the position being posted.

The position, including its job description, will be determined to either be a merit position within the State of Alabama Merit system or an unclassified position. If the position is a position within the State of Alabama Merit System, the hiring manager will follow State of Alabama hiring rules and interview qualified candidates from the state's register for that job class. The hiring managers and HR review and interview qualified applicants, and a decision is made. If the position is outside of the merit system, it will be appropriately approved and the position and job description will be posted internally and on the RSA internet webpage. If an internal candidate is not selected, then external applicants are interviewed. Applicants are screened through various methods, including pre-screening tests, skills assessment, and minimum requirements. As stated above, all applications are tracked through the hiring process. The final hiring decision is made by the hiring manager and Deputy Director. All successful candidates must successfully complete reference checks and criminal background checks before they can be officially appointed or placed into a permanent, temporary, contract employee or onsite contractor position.

Once an employee is hired, they must complete an orientation process where they are informed of RSA policies and procedures related to employee conduct and information security. This process also includes specific job-related training.

## **RISK ASSESSMENT**

RSA maintains a risk assessment process to identify and manage risks that could affect the organization's ability to provide reliable transaction processing for user organizations. The primary objectives of the RSA are delineated in the enabling statutes and specifically include providing retirement and to active and retired members at the least possible cost to taxpayers. Thus, the investment policies are the dominant aspect of planning and risk assessment. The RSA Investment staff and Investment Advisor have quarterly economic update meetings in which they discuss asset allocations and the economic outlook for current and potential investments. RSA periodically reviews and updates financial operating and reporting systems documentation to assist in evaluation and change as may be necessary in controls.

### *Financial Reporting Objectives*

With the strategic plan/annual budget in mind, management identifies, develops and assesses the financial reporting objectives of the organization. Management has a requirement and, therefore, has determined it is appropriate to report its financial statements in accordance with GAAP, including the applicable disclosures. Management believes it has put in place an effective system of controls over financial reporting, which will reflect the underlying transactions of all operating entities in a manner that will provide fairly stated financial statements for the respective entities, when taking into account both qualitative and quantitative materiality considerations.

### *Financial Reporting Risks*

Management, specifically accounting/finance and investment staff, is responsible for identifying and analyzing the risks relative to the achievement of aforementioned financial reporting objectives through the performance of three risk assessments. These risk assessments are:

- Significant Cycle Risk Analysis
- Business Process Risk Assessment
- Information Technology (IT) Risk Assessment

The risk assessments incorporate information derived from various sources, such as:

- Management input
- Previous audit results
- Industry experience and knowledge
- Business/external environment
- Planned system and process changes

The significant cycle risk analysis is a high-level “stop light” analysis of the likelihood and significance of risk as it relates to the achievement of business objectives for each significant cycle, as identified in management’s assessment. Investments and legislative activity have the greatest risk potential for RSA. The investment staff meets with the Investment Advisor for an economic update quarterly and if any adjustments are needed in asset allocation within current authority, they are made. If modifications need to be made in the authorized allocation, then they would be presented to the full Boards. The RSA legislative and finance staff monitor legislative activity and advise the CEO and Legislature of the potential impact of any proposed legislation.

The business process risk assessment is a detailed analysis of the likelihood and significance of risk as it relates to the achievement of specific control objectives within a business cycle. This assessment is performed on a control-by-control basis. Factors considered in this “risk rating” include: the nature and materiality of misstatements that the control is detecting/preventing, inherent risk of account and assertion, volume of transactions, history of errors, interaction with other controls, competency of personnel, complexity of the control, level of automation, and amount of change in the environment. This risk assessment, along with the frequency of occurrence of the controls, drives the testing annually.

#### *Fraud Risks*

The RSA’s Fraud Assessment focuses on the incentives and pressures, attitudes and rationalizations, and opportunities to commit fraud. The risk assessment was performed at two levels: first at the entity-wide level and then during the business process risk assessment, where the RSA explicitly identified controls that mitigated the risk of fraud.

While the RSA cannot eliminate pressures and attitudes, efforts have been made to reduce the opportunities to commit fraud by requiring multiple persons’ involvement in the approval process of financial transactions.

RSA has various tools to assist in the prevention and detection of fraud, such as specific control activities and other monitoring measures that are performed as a normal function of operating the business. Management must and does follow State Ethics law in dealing with independent consultants and other third party service providers.

To address the segregation of duties issues, the RSA has implemented cross-functional peer reviews of various reconciliations and specific risk areas. For instance, Investment accounting/operations personnel do not reconcile their own work to balance to the global custodian.

## **CONTROL OBJECTIVE AND RELATED CONTROL ACTIVITIES**

### **Integration with Risk Assessment**

Along with assessing risks, RSA has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of those objectives.

## **Selection and Development of Control Activities Specified by the Service Organization**

Control activities are a part of the process by which RSA strives to achieve its business objectives. RSA has applied a risk management approach to the organization in order to select and develop control activities. After relevant risk have been identified and evaluated, controls are established, implemented, monitored, reviewed and improved when necessary to meet the overall objectives of the organization.

RSA's control objectives and related control activities are included in Section 4 (the "Testing Matrices") of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in the Testing Matrices. Although the control objectives and related control activities are included in the Testing Matrices, they are, nevertheless, an integral part of RSA's description of the data center services system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in the Testing Matrices, adjacent to the service organization's description of control activities. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

## **MONITORING**

Strict review protocols and division of responsibilities and weekly management meetings to discuss outstanding items and issues provides for real time monitoring of operational activities in the Accounting Department. Regular conference calls and periodic onsite meetings with vendors and client organizations assist in the monitoring process. Senior management is extremely involved in the day to day operations of the RSA and provides for hands on monitoring.

### **On-Going Monitoring**

Management's close involvement in RSA's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of RSA's personnel.

### **Reporting Deficiencies**

Internal tracking tools including reconciliations and trend reports are utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool.

## **INFORMATION AND COMMUNICATION SYSTEMS**

### **Information Systems**

RSA has implemented mechanisms to track and record operational data to make strategic decisions and ensure objectives are consistently achieved. Information gathered from systems enable RSA to understand business trends in order to maximize efforts and provide optimal services.

## Infrastructure

Primary infrastructure used to provide RSA's Pension Administration system includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
Cisco 6500 Series Core Switch	Switch	Network services, performance, and scaling
Cisco Nexus 5k	Switch	Access-layer switches for in-rack deployment
Cisco UCS	Server	VMware host
Dell Servers	Server	VMware host
EMC VNX	SAN storage	Storage
Cisco ISA	Firewall	Firewall Appliance

## Software

Primary software used to provide RSA's Pension Administration system includes the following:

Primary Software	
Software	Purpose
Bloomberg	Application allowing access to the Bloomberg data service, which provides real-time financial data, news feeds, and messages and also facilitates the placement of trades
CAPTAIN	Online corporate action notification, tracking, and response application
CRA Unit Reporting Deposit System	A secure website used by the TRS, ERS, and JRF units to upload the monthly retirement payroll information files
STAARS	General Ledger application used to record transactions for all RSA companies
Library Manager and Work Manager	Member electronic file application where all member correspondence is sent, received, and work flows created (effective 4/2016)
Management Reporter for Microsoft Dynamics ERP	Microsoft application utilized to create, maintain, and view financial statements
Member Online Records	Legacy system, accessed through RSA Workbench for TRS, ERS, and JRF to perform initial enrollment, account maintenance, and distribution processes for members and units
MRI	Application utilized to record Real Estate Office space rental operations
My.StateStreet.com	Internet-based application which allows access to the RSA's safekeeping accounts, including the ability to view, schedule, or download account information, activities, and statements
SunGard APS2	Investment accounting and portfolio management application for securities tracking, regulatory compliance, and report writing
TaxPort Software	Application utilized to maintain 1099 records

<b>Primary Software</b>	
<b>Software</b>	<b>Purpose</b>
The Eze OMS	Global multi-strategy trade order management system (TOMS) that streamlines the investment cycle for all asset classes from idea generation through settlement
Timberline	Application utilized to maintain construction project data
TradeSuite ID (Omgeo)	Application suite that offers automating trade lifecycle events, including allocation, confirmation/affirmation, settlement notification, enrichment, operational analytics, and counterparty risk management between trade counterparties
TradeWeb Web Platform	Online fixed-income trading network that links the trading desks of 35 of the world's leading Fixed-Income dealers
Remote Quick Deposit Program	Regions Bank product used to electronically deposit checks and money orders

### **Communication Systems**

RSA provides regular communication internally to employees and externally to members, participating units, business associates, etc.

In developing internal communications, the appropriate managers work to determine the subject to be communicated and develop key message points to be included in the communication. A wide array of communications is channeled to related parties of RSA that include messages related to HR Policies, Executive Management Messages, Changes in the Operations, Company Mission, Vision, and/or Reporting or Compliance Requirements.

A variety of communications channels are utilized to communicate internally, including meetings as necessary. Communications with the department personnel occurs primarily through email. Similar to the Division/Departmental meetings, senior management meets as necessary.

In addition to the meetings noted above, other communications channels utilized to communicate internally are email, hardcopy publications, and face-to-face meetings. Additionally, the intranet is utilized to distribute key/critical information.

Communication with the Board is maintained through the regularly scheduled meetings noted above. Given the tenure of most board members, a relatively open line of communication exists with the Board.

### **COMPLEMENTARY USER ENTITY CONTROLS**

Controls at RSA cover only a portion of the overall internal control of each user entity. It is not feasible for the control objectives relating to transaction processing to be solely achieved by RSA. Rather, each user entity's internal controls must be evaluated in conjunction with RSA's internal controls.

This section highlights certain internal control responsibilities that RSA believes should be present for each user entity. RSA has considered these in developing its controls described in this report. In order for Client Institutions to rely on the controls reported herein, each Client Institution must evaluate its own internal controls and determine if the following procedures are in place. Furthermore, the controls listed below are intended to address only those control objectives related to the information processing by RSA's systems. Accordingly, this list does not purport to be, and is not, a complete listing of the controls that provide a basis for the assertions underlying a Client Institution's financial statements.

### *Enrollment*

- Units are responsible for the timely dissemination of participant enrollment forms to new employees so that the employees can timely submit them to RSA
- Units are responsible for the timely and accurate submission of the CRA Contribution Remittance forms
- Units are responsible for distributing participant enrollment forms prior to the submission of enrollment data
- Participants are responsible for submitting applicable forms to initiate any changes or updates to their account

### *Valuation*

- Unit management must establish financial reporting processes and controls over the recognition, measurement, presentation and disclosure of its various pension amounts for its financial statement reporting. The unit should have processes and controls in place to determine that complete and accurate information is reported to the plan so that the plan may report census data to the plan actuary regarding active members. Units should have processes and controls in place to promptly review the Annual Statement Listing report provided to participating units by RSA and promptly report errors to RSA benefits department
- Units should have processes and controls in place to promptly review, correct, and certify to RSA the completeness and accuracy of the Annual Checklist sent to the units by RSA of the active members' name, social security number, service and contributions for the annual period under review

### *Contributions*

- Units are responsible for the timely and accurate uploading of contribution information and the timely remittance of funds to RSA
- Units are responsible for ensuring participant's timely and accurate completion of non-enrollee forms, when contributions are received without necessary participant enrollment information
- Units are responsible for the periodic review of the completeness and accuracy of the participant information
- Units are responsible for reporting any changes that need to be made or errors detected in the submission and processing of the enrollment data to RSA
- Participants are responsible for the review of annual statements to verify the accuracy and completeness of their RSA member account information
- Participants are responsible for notifying RSA of any exceptions or errors noted to their account

### *Distributions*

- Units are responsible for certifying complete and accurate termination of employment and last contribution remitted information for distribution requests to RSA as a result of retirement, death of an active or inactive member
- Distribution forms must be submitted by an authorized member of the participant account

### *Information Technology General Controls*

- Units are responsible for maintaining strong passwords, including appropriate password length, complexity, and periodically changing account passwords
- Units and Participants are responsible for keeping user accounts and passwords confidential
- Units are responsible for notifying RSA of any errors when submitting CRA files for processing

## **SECTION 4**

### **TESTING OF CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES PROVIDED BY THE SERVICE AUDITOR**

## **GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR**

A-LIGN's examination of the controls of RSA was limited to the control objectives and related control activities specified by the management of RSA and did not encompass all aspects of RSA's operations or operations at user organizations. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No. 16 (SSAE 16).

Our examination of the control activities was performed using the following testing methods:

<b>TEST</b>	<b>DESCRIPTION</b>
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether a SSAE 16 report meets the user auditor's objectives, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the processing of the user organization's transactions
- Understand the flow of significant transactions through the service organization
- Determine whether the control objectives are relevant to the user organization's financial statement assertions
- Determine whether the service organization's controls are suitably designed to prevent or detect processing errors that could result in material misstatements in the user organization's financial statements and determine whether they have been implemented

**CONTROL AREA 1                      PHYSICAL SECURITY**

Control Objective Specified by the Service Organization:      Controls provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage, and interference.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.1	Documented physical security policies and procedures are in place to guide personnel in physical security administration.	Inspected the security policies and procedures to determine that documented physical security policies and procedures were in place to guide personnel in physical security administration.	No exceptions noted.
1.2	A surveillance system is in place to monitor and record activity for facility entrances, internal access points, and key areas throughout the facility.	Observed the surveillance system monitoring dashboard to determine that a surveillance system was in place to monitor and record activity for facility.  Inspected video footage for a sample of days to determine that a surveillance system was in place to monitor and record activity for facility entrances, internal access points, and key areas throughout the facility.	No exceptions noted.  No exceptions noted.
1.3	Access to the datacenter is restricted by a card scan system and authorized badge access to the facilities 4 <sup>th</sup> floor. Visitors to the datacenter are required to sign-in using a visitor’s log to track the date, time, and individual requesting access.	Observed the card scan system and required badge access in the elevator to determine that access to the datacenter was restricted by a card scan system and authorized badge access to the facilities 4 <sup>th</sup> floor.  Inspected the datacenter visitor logs for a sample of months to determine that visitors to the datacenter were required to sign-in using a visitor’s log to track the date, time, and individual requesting access.	No exceptions noted.  No exceptions noted.
1.4	Employees are assigned badge access privileges to the facility through the use of predefined access zones based on their job function. Physical keys are distributed to management personnel, and the key log is maintained by the Security group.	Inquired of the Head of Security regarding badge access privileges to determine that employees were assigned badge access privileges to the facility through the use of predefined access zones based on their job function and that physical keys were distributed to management personnel, and the key log was maintained by the Security group.	No exceptions noted.

**CONTROL AREA 1                      PHYSICAL SECURITY**

Control Objective Specified by the Service Organization:      Controls provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage, and interference.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the badge access privileges, badge access zone configurations, and the physical key log to determine that employees were assigned badge access privileges to the facility through the use of predefined access zones based on their job function and that physical keys were distributed to management personnel, and the key log was maintained by the Security group.	No exceptions noted.
1.5	The badge access system is configured to log badge access attempts. Access logs can be traced to specific days and access cards.	Inspected the badge access log for a sample of days to determine that the badge access system was configured to log badge access attempts and that access logs could be traced to specific days and access cards.	No exceptions noted.
1.6	The facilities are protected with a centralized panic alarm system that is monitored by a 24/7 alarm monitoring company.	Inspected the alarm monitoring invoice for a sample of months to determine that the facilities were protected with a centralized panic alarm system that was monitored by a 24/7 alarm monitoring company.	No exceptions noted.
1.7	Visitors entering the RSA Headquarters are met by a security guard and must be escorted to the appropriate department by an authorized RSA employee. All access doors throughout the facility are locked and secured by an access card scanning system which helps prevent entry by unauthorized individuals.	Observed the security processes to determine that visitors entering the RSA Headquarters were met by a security guard and were escorted to the appropriate department by an authorized RSA employee and that all access doors throughout the facility were locked and secured by an access card scanning system which helped prevent entry by unauthorized individuals.	No exceptions noted.

**CONTROL AREA 2**

**ENVIRONMENTAL SAFEGUARDS**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.1	A diesel power generator is in place to provide electricity to the onsite data center in the event of a power outage.	<p>Observed the diesel power generator to determine that a diesel power generator was in place to provide electricity to the onsite data center in the event of a power outage.</p> <p>Inspected diesel power generator maintenance contract and diesel fuel contract to determine that a diesel power generator was in place to provide electricity to the onsite data center in the event of a power outage.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
2.2	Fire detection and suppression systems are installed throughout the facility and data center.	Observed the fire detection and suppression equipment to determine that fire detection and suppression systems were installed throughout the facility and data center.	No exceptions noted.
2.3	Production equipment is maintained in racks to protect the equipment from localized flooding and facilitate cooling.	Observed the production equipment racks to determine that production equipment was maintained in racks to protect the equipment from localized flooding and facilitate cooling.	No exceptions noted.
2.4	The facility and server room is equipped with multiple air conditioning units to help regulate temperature within the server room.	Observed the air conditioning units to determine that the facility and server room was equipped with multiple air conditioning units to help regulate temperature within the server room.	No exceptions noted.
2.5	The generator is powered up and tested weekly to confirm that the generator is functioning as expected.	Inspected the generator test log for a sample of weeks to determine that the generator was powered up and tested weekly to confirm that the generator was functioning as expected.	No exceptions noted.

**CONTROL AREA 2****ENVIRONMENTAL SAFEGUARDS**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats.

<b>Control Point</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
2.6	The onsite data center is equipped with a humidity monitoring and water detection system to alert IT personnel if excessive humidity or water is detected.	Observed the onsite data center humidity monitoring and water detection units to determine that the onsite data center was equipped with a humidity monitoring and water detection system to alert IT personnel if excessive humidity or water was detected.	No exceptions noted.
2.7	Third party specialists inspect and maintain air conditioning units on a periodic basis.	Inspected the inspection logs for a sample of quarters to determine that third party specialists inspected and maintained the air conditioning units on a periodic basis.	No exceptions noted.
2.8	Third party specialists inspect and maintain fire detection and suppression equipment on an annual basis.	Inspected the fire alarm and fire suppression annual maintenance reports to determine that third party specialists inspected and maintained the fire detection and suppression equipment on an annual basis.	No exceptions noted.

**CONTROL AREA 3                      COMPUTER OPERATIONS - BACKUP**

Control Objective Specified by the Service Organization:      Controls provide reasonable assurance of timely system backups of critical files, off-site backup storage, and regular off-site rotation of backup files (if backups are to physical media).

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.1	IT personnel utilize documented backup and recovery procedures to help ensure that backups are performed.	Inspected the backup policy and recovery procedures to determine that IT personnel utilized documented backup and recovery procedures to help ensure that backups were performed.	No exceptions noted.
3.2	SQL servers are supported by various maintenance plans that are configured on each database server and provide a mechanism for back up and verification alerts if any part of the verification fails or has anomalies.	Inspected the maintenance plan configurations and an example verification alert to determine that SQL servers were supported by various maintenance plans that were configured on each database server and provided a mechanism for back up and verification alerts if any part of the verification failed or had anomalies.	No exceptions noted.
3.3	An automated backup process is configured to backup production servers and data on a daily basis.	Inspected the backup policy and automated backup job summary schedules to determine that an automated backup process was configured to backup production servers and data on a daily basis.	No exceptions noted.
3.4	Management protects sensitive information - logically and physically, in storage and during transmission against unauthorized access or modification.	<p>Inquired of the Security &amp; Infrastructure Manager regarding the protection of sensitive information to determine that management protected sensitive information - logically and physically in storage and during transmission against unauthorized access or modification.</p> <p>Inspected the backup software encryption configuration and access restrictions to backup software to determine that management protected sensitive information - logically and physically in storage and during transmission against unauthorized access or modification.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

**CONTROL AREA 3****COMPUTER OPERATIONS - BACKUP**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance of timely system backups of critical files, off-site backup storage, and regular off-site rotation of backup files (if backups are to physical media).

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.5	Production system backups of RSA Workbench System data are performed by on-demand computer operator jobs daily and backed up to the Data Domain Commvault system. Management receives a daily backup status notification when backups are completed successfully or unsuccessfully.	Inspected the computer operator job configuration and backup summary reports for a sample of days to determine that production system backups of RSA Workbench System data were performed by on-demand computer operator jobs daily and backed up to the Data Domain Commvault system and that management received a daily backup status notification when backups were completed successfully or unsuccessfully.	No exceptions noted.
3.6	RSA uses Data Domain and EMC Avamar devices that provide deduplication between the main datacenter, the Dexter datacenter, and the data center in Mobile.	Inspected the replication configurations and activity logs for a sample of days to determine that RSA used Data Domain and EMC Avamar devices that provided deduplication between the main datacenter, the Dexter datacenter, and the data center in Mobile.	No exceptions noted.
3.7	Restores are performed on a random selection of SQL server databases once every two weeks.	Inspected the restore configurations and restore activity results for a sample of weeks to determine that restores were performed on a random selection of SQL server databases once every two weeks.	No exceptions noted.

**CONTROL AREA 4                      COMPUTER OPERATIONS - AVAILABILITY**

Control Objective Specified by the Service Organization:      Controls provide reasonable assurance that systems are maintained in a manner that helps ensure system availability.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.1	Incident response policies and procedure are in place to guide personnel in reporting and responding to major information technology incidents.	Inspected the incident response policies and procedures to determine that incident response policies and procedure were in place to guide personnel in reporting and responding to major information technology incidents.	No exceptions noted.
4.2	Patch monitoring and distribution policies and procedures are in place to guide personnel in the patch management processes and updates.	Inspected the patch monitoring documented policies and procedures to determine that patch monitoring and distribution policies and procedures were in place to guide personnel in the patch management processes and updates.	No exceptions noted.
4.3	An incident ticket management system is in place to assign, track, and monitor operational incidents.	Inspected the operational incidents in the incident ticket management system and the incident ticket management system configuration to determine that an incident ticket management system was in place to assign, track, and monitor operational incidents.	No exceptions noted.
4.4	An enterprise monitoring application is configured to monitor performance and capacity requirements and to send e-mail notifications for identified issues.	Inspected the enterprise monitoring application configurations and internal scripts to determine that an enterprise monitoring application was configured to monitor performance and capacity requirements and to send e-mail notifications for identified issues.	No exceptions noted.
4.5	Antivirus software is installed on servers and workstations and is configured to update virus definitions every ten minutes and to perform scheduled server and laptop scans on a daily basis and desktop scans twice per week.	Inspected the antivirus software configurations to determine that antivirus software was installed on servers and workstations and was configured to update virus definitions every ten minutes and to perform scheduled server and laptop scans on a daily basis and desktop scans twice per week.	No exceptions noted.

**CONTROL AREA 4                    COMPUTER OPERATIONS - AVAILABILITY**

Control Objective Specified by the Service Organization:    Controls provide reasonable assurance that systems are maintained in a manner that helps ensure system availability.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.6	Network vulnerability and malware scans are performed and assessment results reviewed by operations personnel.	Inspected the most recent vulnerability assessment and penetration test performed by a third party to determine that network vulnerability and malware scans were performed and assessment results reviewed by operations personnel.	No exceptions noted.
4.7	Service contracts are in place with third party vendors to support production hardware and software.	Inspected the service contracts for a sample of third party vendors to determine that service contracts were in place with third party vendors to support production hardware and software.	No exceptions noted.

**CONTROL AREA 5                      DATA COMMUNICATION**

Control Objective Specified by the Service Organization:      Controls provide reasonable assurance that data maintains its integrity and security as it is transmitted between third parties and the service organization.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.1	Firewall systems are in place at the network perimeter to filter unauthorized inbound traffic from the Internet.	<p>Inquired of the Security &amp; Infrastructure Manager regarding firewall systems to determine that firewall systems were in place at the network perimeter to filter unauthorized inbound traffic from the Internet.</p> <p>Inspected the documented policies and procedures, network diagram, and the firewall system configurations to determine that firewall systems were in place at the network perimeter to filter unauthorized inbound traffic from the Internet.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
5.2	Management protects sensitive information - logically and physically, during transmission against unauthorized access or modification.	Inspected the file transfer encryption configuration and schedules to determine that management protected sensitive information - logically and physically, during transmission against unauthorized access or modification.	No exceptions noted.
5.3	Management restricts the ability to administer the firewall system to the appropriate IT personnel.	<p>Inquired of the Security &amp; Infrastructure Manager regarding the Access Control Server (ACS) network domain administrator access rights to determine that management restricted the ability to administer the firewall system to the appropriate IT personnel.</p> <p>Inspected the firewall administrator access listing to determine that management restricted the ability to administer the firewall system to the appropriate IT personnel.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
5.4	Remote users are authenticated via an authorized user account and password before being granted access to the systems.	Inquired of the Security & Infrastructure Manager regarding remote user authentication to determine that remote users were authenticated via an authorized user account and password before being granted access to the systems.	No exceptions noted.

**CONTROL AREA 5**

**DATA COMMUNICATION**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that data maintains its integrity and security as it is transmitted between third parties and the service organization.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.5	The firewall system is configured to deny general access and permit access based on IP address.	<p>Inspected the virtual private network (VPN) configuration and VPN access rights to determine that remote users were authenticated via an authorized user account and password before being granted access to the systems.</p> <p>Inquired of the Security &amp; Infrastructure Manager regarding the firewall system configuration to determine that the firewall system was configured to deny general access and permit access based on IP address.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
5.6	The firewall system requires administrators to authenticate via an authorized user account and password prior to performing administration tasks.	<p>Inspected the firewall system configurations to determine that the firewall system was configured to deny general access and permit access based on IP address.</p> <p>Inquired of the Security &amp; Infrastructure Manager regarding the firewall system administrator authentication to determine that the firewall system required administrators to authenticate via an authorized user account and password prior to performing administration tasks.</p> <p>Inspected the firewall login dashboard and the firewall administrator access listing to determine that the firewall system required administrators to authenticate via an authorized user account and password prior to performing administration tasks.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

**CONTROL AREA 6                      INFORMATION SECURITY**

Control Objective Specified by the Service Organization:      Controls provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition, or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.1	Information security policies and procedures are in place to guide personnel in managing system access and protecting information assets and data.	Inspected the Information Security policies and procedures to determine that information security policies and procedures were in place to guide personnel in managing system access and protecting information assets and data.	No exceptions noted.
6.2	Administrator access within the network domain is restricted to authorized individuals.	Inquired of the Security & Infrastructure Manager regarding administrator access rights to determine that administrator access within the network domain was restricted to authorized individuals.	No exceptions noted.
6.3	<p>Application users are authenticated via an authorized user account and password before being granted access to the application. The application is configured to enforce the following password requirements:</p> <ul style="list-style-type: none"> <li>• Enforce password history</li> <li>• Maximum password age</li> <li>• Minimum password length</li> <li>• Password must meet complexity requirements</li> <li>• Account lockout</li> </ul>	<p>Inspected the listing of administrators on the network domain to determine that administrator access within the network domain was restricted to authorized individuals.</p> <p>Inspected the user authentication requirements and password policy configuration to determine that application users were authenticated via an authorized user account and password before being granted access to the application and that the application was configured to enforce the following password requirements:</p> <ul style="list-style-type: none"> <li>• Enforce password history</li> <li>• Maximum password age</li> <li>• Minimum password length</li> <li>• Password must meet complexity requirements</li> <li>• Account lockout</li> </ul>	No exceptions noted.

**CONTROL AREA 6                      INFORMATION SECURITY**

Control Objective Specified by the Service Organization:      Controls provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition, or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.4	Management reviews the access rights of employees on an annual basis.	Inspected the role change list, permission reviews and system access reviews to determine that management reviewed the access rights of employees on an annual basis.	No exceptions noted.
6.5	Network based intrusion software monitors network traffic to critical devices.	Inspected the enterprise monitoring and network intrusion software configurations and an example report to determine that network based intrusion software monitored network traffic to critical devices.	No exceptions noted.
6.6	<p>Network users are authenticated via an authorized user account and password before being granted access to the network domain. The network domain is configured to enforce the following password requirements:</p> <ul style="list-style-type: none"> <li>• Enforce password history</li> <li>• Maximum password age</li> <li>• Minimum password length</li> <li>• Password must meet complexity requirements</li> </ul>	<p>Inspected the network user authentication requirements and password policy configuration to determine that network users were authenticated via an authorized user account and password before being granted access to the network domain and that the network domain was configured to enforce the following password requirements:</p> <ul style="list-style-type: none"> <li>• Enforce password history</li> <li>• Maximum password age</li> <li>• Minimum password length</li> <li>• Password must meet complexity requirements</li> </ul>	No exceptions noted.
6.7	Systems administration personnel activate user accounts based on authorized access requests as a component of the hiring process.	Inspected the new hire documentation for a sample of new hires to determine that systems administration personnel activated user accounts based on authorized access requests as a component of the hiring process.	No exceptions noted.

**CONTROL AREA 6                      INFORMATION SECURITY**

Control Objective Specified by the Service Organization:      Controls provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition, or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.8	Systems administration personnel deactivate user accounts assigned to terminated employees as a component of the termination process.	Inspected the network and application user access listings and termination documentation for a sample of terminated employees to determine that systems administration personnel deactivated user accounts assigned to terminated employees as a component of the termination process.	No exceptions noted.
6.9	User accounts are assigned to predefined access roles to restrict access to certain functions within the applications.	<p>Inquired of the Security &amp; Infrastructure Manager regarding access roles to determine that user accounts were assigned to predefined access roles to restrict access to certain functions within the applications.</p> <p>Inspected the system-generated application access listing to determine that user accounts were assigned to predefined access roles to restrict access to certain functions within the applications.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

**CONTROL AREA 7****CHANGE MANAGEMENT**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that changes to production environments are authorized, communicated, verified, and documented to minimize service interruption.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.1	Access to promote changes into production is limited to IT System Administrators.	Inquired of the Security & Infrastructure Manager regarding users with access to production to determine that access to promote changes into production was limited to IT System Administrators.  Inspected a sample of changes and a list of users with access to production to determine that access to promote changes into production was limited to IT System Administrators.	No exceptions noted.  No exceptions noted.
7.2	Changes are authorized by members of the ITS management prior to the initiation of any change development.	Inspected a sample of changes to determine that changes were authorized by members of the ITS management prior to the initiation of any change development.	No exceptions noted.
7.3	Changes are approved by members of the ITS change management group prior to promotion of the changes into production.	Inspected a sample of changes to determine that changes were approved by members of the ITS change management group prior to promotion of the changes into production.	No exceptions noted.
7.4	Changes are tested within a development and test environment prior to promotion into production. Development and testing procedures are approved by ITS management.	Inspected a sample of changes to determine that changes were tested within a development and test environment prior to promotion into production and that development and testing procedures were approved by ITS management.	No exceptions noted.

**CONTROL AREA 8                      ENROLLMENT**

Control Objective Specified by the Service Organization:      Control activities provide reasonable assurance that member information is recorded completely, accurately and timely.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
8.1	New enrollment forms are required to be completed as part of the new member enrollment process. Where a new member enrollment form is not submitted, the employer must submit necessary new member data as part of the contribution process.	Inspected the completed enrollment forms for a sample of new members to determine that new enrollment forms were required to be completed as part of the new member enrollment process and that where a new member enrollment form was not submitted, the employer must submit necessary new member data as part of the contribution process.	No exceptions noted.
8.2	Enrollment forms are processed through the Library Manager workflow system to help ensure the forms are processed completely and in a timely fashion. Incomplete enrollment forms are automatically routed to a queue to be resolved by the TRS or ERS Benefits Departments.	Observed the submission of a complete and incomplete enrollment form to determine that enrollment forms were processed through the Library Manager workflow system to help ensure the forms were processed completely and in a timely fashion and that incomplete enrollment forms were automatically routed to a queue to be resolved by the TRS or ERS Benefits Departments.	No exceptions noted.
8.3	Library Manager requires a secondary review of new enrollment data by an operator of Office Services.	<p>Inspected a workflow log processed through Library Manager to determine that Library Manager required a secondary review of new enrollment data by an operator of Office Services.</p> <p>Observed a new enrollment processed through Library Manager to determine that Library Manager required a secondary review of new enrollment data by an operator of Office Services.</p>	No exceptions noted.
8.4	Members of Office Services process new enrollments within Library Manager on a timely basis.	Inspected the Library Manager workflow log to determine that members of Office Services processed new enrollments within Library Manager on a timely basis.	No exceptions noted.

**CONTROL AREA 8            ENROLLMENT**

Control Objective Specified by the Service Organization:    Control activities provide reasonable assurance that member information is recorded completely, accurately and timely.

<b>Control Point</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
8.5	Access to update new enrollment data within the workbench system is limited to appropriate personnel.	Inspected a list of users with access to the workbench system to determine that access to update new enrollment data within the workbench system was limited to appropriate personnel.	No exceptions noted.

**CONTROL AREA 9**

**CONTRIBUTIONS**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that contributions received and posted to member accounts are complete and accurate.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
9.1	Accounting restrictively endorses contribution checks upon receipt and deposits cash receipts daily and controls access to receipts by storing them in a secure cabinet to prevent unauthorized access to cash receipts and to prevent unrecorded cash receipts.	Observed the handling of cash receipts for a day's deposits by a Revenue Accounting Clerk to determine that accounting restrictively endorsed contribution checks upon receipt and deposited cash receipts daily and controlled access to receipts by storing them in a secure cabinet to prevent unauthorized access to cash receipts and to prevent unrecorded cash receipts.	No exceptions noted.
9.2	Contribution requirements and limitations are described in the law and monitored by RSA staff.	Inspected the policy documentation regarding contribution requirements to determine that contribution requirements and limitations were described in the law and monitored by RSA staff.	No exceptions noted.
9.3	Contributions posted must be from an approved unit with a valid contribution code.	<p>Inquired of the Director of Revenue regarding the process of receiving contributions to determine that contributions posted were from an approved unit with a valid contribution code.</p> <p>Inspected the file upload requirements and screenshots of a contribution file upload to determine that contributions posted were from an approved unit with a valid contribution code.</p>	No exceptions noted.
9.4	Accounting reviews the clerical accuracy of the contribution forms and the cash receipt amounts are reviewed for completeness and accuracy before funds are posted to member accounts. The control total (remittance amount) is reconciled to the total member contributions amount.	Observed the Revenue Accounting clerk verify the balances per the CRA file review to determine that accounting reviewed the clerical accuracy of the contribution forms and that the cash receipt amounts were reviewed for completeness and accuracy before funds were posted to member accounts and that the control total remittance amount was reconciled to the total member contributions amount.	No exceptions noted.

**CONTROL AREA 9**

**CONTRIBUTIONS**

Control Objective Specified by the Service Organization:

Control activities provide reasonable assurance that contributions received and posted to member accounts are complete and accurate.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected a sample of contribution forms to determine that accounting reviewed the clerical accuracy of the contribution forms and that the cash receipt amounts were reviewed for completeness and accuracy before funds were posted to member accounts and that the control total remittance amount was reconciled to the total member contributions amount.	No exceptions noted.
9.5	The day after a deposit, an RSA Revenue Accounting Clerk will ensure that the funds were correctly posted for the prior days' ERS and TRS receipts.	Inspected a sample of reconciliations performed to determine that the day after a deposit, a RSA Revenue Accounting Clerk would ensure that the funds were correctly posted for the prior days' ERS and TRS receipts.	No exceptions noted.
9.6	A daily roll-forward from the prior day's ledger balance is performed by the Revenue Accounting department to ensure that the funds were correctly posted for the prior day's JRF receipts.	Inspected the daily roll-forward for a sample of days to determine that a daily roll-forward from the prior day's ledger balance was performed by the Revenue Accounting department to ensure that the funds were correctly posted for the prior day's JRF receipts.	No exceptions noted.
9.7	The RSA Revenue Accounting Department runs a Past Due Contributions Report listing units that have not uploaded and remitted the required monthly contribution to help ensure that members are receiving the appropriate credit for amounts withheld from unit payrolls.	Inspected a sample of monthly past due contributions reports to determine that the RSA Revenue Accounting Department ran a Past Due Contributions report listing units that had not uploaded and remitted the required monthly contribution to help ensure that members were receiving the appropriate credits for amounts withheld from unit payrolls.	No exceptions noted.

**CONTROL AREA 10                      DISTRIBUTIONS**

Control Objective Specified by the Service Organization:      Control activities provide reasonable assurance that distributions are complete and accurate and in accordance with plan rules and participant instructions and are properly recorded in member’s accounts.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
10.1	There is adequate segregation of duties within the member online system and only ERS/TRS/ and JRF Benefit departments have the access to make changes to member accounts that impact benefit payments. The Member Payroll group that processes the benefit payments do not have the access to make changes that would impact benefit payments.	Inspected the members’ online system control list to determine that there was adequate segregation of duties within the member online system and that only ERS/TRS/ and JRF Benefit departments had access to make changes to member accounts that impact benefit payments and that the Member Payroll group that processed the benefit payments did not have the access to make changes that would impact benefit payments.	No exceptions noted.
10.2	When a member terminates from service and withdraws their account balance before retirement eligible, they must submit a Notice of Final Deposit and Request for Refund which certifies their termination of service. The Benefits department will update the member’s account and send a Withdrawal Payroll worksheet to the Member Payroll group who will complete the process of distributing the appropriate balance of the member’s account. The Member Payroll group then compares the amount of the benefit per the Withdrawal Payroll worksheet with the information in the refund menu of the RSA workbench to help ensure accuracy of the refund payment.	Inspected a sample of Contact Service forms for a sample of accounts for which the members withdrew and requested a refund during the review period to determine that when a member terminated from service and withdrew from service, they submitted a Notice of Final Deposit and Request for Refund which certified their termination of service and that the Benefits department updated the members account and sent a Withdrawal Payroll worksheet to the Member Payroll group who completed the process of distributing the appropriate balance of the member’s account and that the Member Payroll group then compared the amount of the benefit per the Withdrawal Payroll Worksheet with the information on the refund menu of the RSA workbench to help ensure the accuracy of the payment.	No exceptions noted.

**CONTROL AREA 10            DISTRIBUTIONS**

Control Objective Specified by the Service Organization:    Control activities provide reasonable assurance that distributions are complete and accurate and in accordance with plan rules and participant instructions and are properly recorded in member’s accounts.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
10.3	As the Benefits personnel add individuals to the supplemental payroll, they prepare worksheets for Member Payroll. Member Payroll personnel then collect these worksheets from the Benefits Department. Member Payroll accountants compare the worksheets to the information in the Member Online System for clerical accuracy and completeness.	Inspected a sample of worksheets for a sample of members receiving supplemental payments to determine that as the Benefits personnel added individuals to the supplemental payroll, they prepared worksheets for Member Payroll and that member Payroll personnel then collected these worksheets from the Benefits department and member payroll accountants compared the worksheets to the information in the Member Online System for clerical accuracy and completeness.	No exceptions noted.
10.4	The final Daily Reconciliation Report for the week is compared to the weekly Payroll report by Accounting Clerks, and any discrepancies are investigated. Two individuals with signature authority (Authorized Voucher Signors as documented by RSA) are needed to approve the Payroll Report.	Inspected the weekly Payroll Report and corresponding final Daily Reconciliation Report for a sample of weeks to determine that the final Daily Reconciliation Report for the week was compared to the Payroll Report by Accounting Clerks, and any discrepancies were investigated and that two individuals with authority (Authorized Voucher Signors as documented by RSA) were needed to approve the Payroll Report.	No exceptions noted.
10.5	The weekly benefit checks are counted by Member Payroll Personnel and the total is compared to the number of checks per the payroll report to ensure completeness.	Inspected the payroll reports for a sample of weeks to determine that the weekly benefit checks were counted by member Payroll Personnel and the total number was compared to the number of checks per the payroll report to ensure completeness.	No exceptions noted.

**CONTROL AREA 10                    DISTRIBUTIONS**

Control Objective Specified by the Service Organization:      Control activities provide reasonable assurance that distributions are complete and accurate and in accordance with plan rules and participant instructions and are properly recorded in member’s accounts.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
10.6	After the monthly benefits payroll is run, the File Balance Report is generated and balanced to the corresponding spreadsheet for both the regular retiree monthly payroll and the monthly DROP payroll. Two individuals with signature authority (Authorized Voucher Signors as documented by RSA) approve the monthly benefit payrolls.	Inspected the File Balance Report and the corresponding spreadsheet for both the regular retiree monthly payroll and the monthly DROP register for a sample of months to determine that after the monthly payroll was run, the File Balance Report was generated and balanced to the corresponding spreadsheet for both the regular retiree monthly payroll and the monthly DROP register and that two individuals (Authorized Voucher Signors as documented by RSA) approved the monthly benefit payrolls.	No exceptions noted.
10.7	Balancing reports are run monthly beginning in the third quarter of a calendar year to identify errors for correction prior to preparing the 1099s at the end of the year.	Inspected the balancing reports for a sample of months and the related reconciliations performed by the payroll accounting department to determine that balancing reports were run monthly beginning in the third quarter of a calendar year to identify errors for correction prior to preparing the 1099s at the end of the year.	No exceptions noted.
10.8	After retirement payments are finalized, a Payroll Summary is prepared by Member Payroll Personnel and delivered to the retirement plan’s management for review.	<p>Inquired of the Member Payroll Manager regarding management oversight of the monthly payroll process to determine that after retirement payments were finalized, a Payroll Summary was prepared by Member Payroll Personnel and delivered to the retirement plan’s management for review.</p> <p>Inspected the monthly payroll summary for a sample of months to determine that after retirement payments were finalized, a Payroll Summary was prepared by Member Payroll Personnel and delivered to the retirement plan’s management for review.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

**CONTROL AREA 11            ERS/TRS/JRF - VALUATION**

Control Objective Specified by the Service Organization:    Control activities provide reasonable assurance that the annual plan valuation and underlying census data is accurately reported.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
11.1	Current year totals of the following items: <ul style="list-style-type: none"> <li>• Total count of active and inactive members</li> <li>• Total count of withdrawn members by type</li> <li>• Total amount of compensation for active members</li> <li>• The number of retirees by account status</li> <li>• The number of retirees by retirement type is compared to prior year totals to test and verify the completeness of the current year files</li> </ul>	Inspected the RSA schedules provided to the third-party actuary to determine that current year totals of the following items: <ul style="list-style-type: none"> <li>• Total count of active and inactive members</li> <li>• Total count of withdrawn members by type</li> <li>• Total amount of compensation for active members</li> <li>• The number of retirees by account status</li> <li>• The number of retirees by retirement type were compared to prior year totals to test and verify the completeness of the current year files</li> </ul>	No exceptions noted.
11.2	The valuation file data for the following items: <ul style="list-style-type: none"> <li>• Member contributions per the valuation file</li> <li>• Makeup/purchased service contributions per the valuation file</li> <li>• Ending annuity savings fund amount per the valuation file</li> <li>• Regular withdrawal amounts per the valuation file</li> <li>• Death withdrawal amounts per the valuation file</li> <li>• Amounts transferred out for retirement per the valuation file is compared to the general ledger accounts at fiscal year-end to test the accuracy and completeness of the valuation file data</li> </ul>	Inspected the documentation provided to the third-party actuary to determine that the valuation of the data for the following items: <ul style="list-style-type: none"> <li>• Member contributions per the valuation file</li> <li>• Makeup/purchased service contributions per the valuation file</li> <li>• Ending annuity savings fund amount per the valuation file</li> <li>• Regular withdrawal amounts per the valuation file</li> <li>• Death withdrawal amounts per the valuation file</li> <li>• Amounts transferred out for retirement per the valuation file was compared to the general ledger accounts at fiscal year-end to test the accuracy and completeness of the valuation data</li> </ul>	No exceptions noted.



**CONTROL AREA 11                      ERS/TRS/JRF - VALUATION**

Control Objective Specified by the Service Organization:      Control activities provide reasonable assurance that the annual plan valuation and underlying census data is accurately reported.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
11.4	<p>Analytical review procedures are performed to test the accuracy and completeness of the actuarial valuation files. Additional procedures performed include:</p> <ul style="list-style-type: none"> <li>• Comparing the calculated death benefit, administrative expense, and term life (TRS only) amounts based on the compensation in valuation file to the general ledger account balances</li> <li>• Checking that employment and withdrawal dates are included throughout the fiscal year and that there are none after fiscal year-end</li> <li>• Identifying unreasonable dates of birth, employment dates, etc.</li> <li>• Comparing count of retirees/beneficiaries receiving benefits per the valuation file to the count maintained by Accounting Payroll Check that retirement dates are included throughout the fiscal year and that there are no retirement dates included after fiscal year-end</li> <li>• Checking that retirement dates are included throughout the fiscal year and that there are no retirement dates included after fiscal year-end</li> <li>• Identifying unreasonable dates of birth, retirement dates, etc., investigate, and correct if necessary</li> </ul>	<p>Inspected the analytical calculations within the documentation provided to the third-party actuary to determine that analytical review procedures were performed to test the accuracy and completeness of the actuarial valuation files and that additional procedures performed included:</p> <ul style="list-style-type: none"> <li>• Comparing the calculated death benefit, administrative expense, and term life (TRS only) amounts based on the compensation in valuation file to the general ledger account balances</li> <li>• Checking that employment and withdrawal dates are included throughout the fiscal year and that there are none after fiscal year-end</li> <li>• Identifying unreasonable dates of birth, employment dates, etc.</li> <li>• Comparing count of retirees/beneficiaries receiving benefits per the valuation file to the count maintained by Accounting Payroll</li> <li>• Check that retirement dates are included throughout the fiscal year and that there are no retirement dates included after fiscal year-end</li> <li>• Checking that retirement dates are included throughout the fiscal year and that there are no retirement dates included after fiscal year-end</li> <li>• Identifying unreasonable dates of birth, retirement dates, etc., investigate, and correct if necessary</li> </ul>	No exceptions noted.

**CONTROL AREA 11**

**ERS/TRS/JRF - VALUATION**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the annual plan valuation and underlying census data is accurately reported.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
11.5	DROP (Deferred Retirement Option Program) file testing includes: <ul style="list-style-type: none"> <li>• Selecting a sample from the actuarial valuation files and the data is compared to the member’s fiscal year-end statement from the RSA System to verify the accuracy of the file data</li> <li>• Comparing Valuation file data to the general ledger accounts at fiscal year-end to test the reasonableness of the valuation file data including DROP contributions, benefits, interest distributions, forfeitures, and beginning and ending DROP equity</li> </ul>	Inspected the DROP (Deferred Retirement Option Program) file testing to determine that DROP file testing included: <ul style="list-style-type: none"> <li>• Selecting a sample from the actuarial valuation files and the data is compared to the member’s fiscal year-end statement from the RSA System to verify the accuracy of the file data</li> <li>• Comparing Valuation file data to the general ledger accounts at fiscal year-end to test the reasonableness of the valuation file data including DROP contributions, benefits, interest distributions, forfeitures, and beginning and ending DROP equity</li> </ul>	No exceptions noted.
11.6	Actuarial valuation data files are sent to the actuary upon approval by RSA’s CFO.	Inspected the documented approval by the CFO to determine that actuarial valuation data files were sent to the actuary upon approval by RSA’s CFO.	No exceptions noted.
11.7	Actuarial valuation data files sent to the actuaries are encrypted and password protected.	Inspected the email encryption codes to determine that actuarial valuation data files sent to the actuaries were encrypted and password protected.	No exceptions noted.
11.8	Upon completion of the valuations, the actuaries provide RSA with preliminary results including draft actuarial valuation reports for ERS, TRS, and JRF. The draft copies are reviewed by RSA Accounting staff and RSA CFO.	Inspected the reviews of the actuarial documentation performed by RSA to determine that upon completion of the valuations, the actuaries provided RSA with preliminary results including draft actuarial valuation reports for ERS, TRS, and JRF, and that the draft copies were reviewed by RSA Accounting staff and RSA CFO.	No exceptions noted.

**CONTROL AREA 11            ERS/TRS/JRF - VALUATION**

Control Objective Specified by the Service Organization:    Control activities provide reasonable assurance that the annual plan valuation and underlying census data is accurately reported.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
11.9	<p>Annually after the plan year end, participating RSA units are provided an Annual Checklist detailing the contribution amounts, assigned tier and service credit for their employees for the preceding plan year. Participating TRS units are required to return these and certify to their accuracy and completeness and indicate any discrepancies so that RSA staff can make appropriate corrections.</p>	<p>Inspected a sample of TRS units and requested the related returned checklists to determine that annually, after the plan year end, participating TSA units were provided an Annual Checklist detailing the contribution amounts, assigned tier and service credit for their employees for the preceding plan year and that participating TRS units were required to return these and certify to their accuracy and completeness and indicate any discrepancies so that RSA staff can make appropriate corrections.</p>	<p>No exceptions noted.</p>
11.10	<p>RSA's auditors select a representative group of TRS contributing employers and test underlying payroll and census data for employees who are potentially eligible for participation in the TRS plan. Contributing employers are subject to testing on the following basis:</p> <ul style="list-style-type: none"> <li>• Employers constituting more than 20 percent of contributions are tested annually</li> <li>• Employers constituting at least 5% of contributions are tested on a five-year cycle</li> <li>• Employers constituting at least 2 percent are tested on a ten-year cycle</li> </ul>	<p>Inspected the TRS allocation documentation provided by the Chief Financial Officer of RSA to determine that RSA's auditors selected a representative group of TRS contributing employers and tested underlying payroll and census data for employees who were potentially eligible for participation in the TRS plan and that contributing employers were subject to testing on the following basis:</p> <ul style="list-style-type: none"> <li>• Employers constituting more than 20 percent of contributions were tested annually</li> <li>• Employers constituting at least 5% of contributions were tested on a five-year cycle</li> <li>• Employers constituting at least 2 percent were tested on a ten-year cycle</li> </ul>	<p>No exceptions noted.</p>

**CONTROL AREA 11            ERS/TRS/JRF - VALUATION**

Control Objective Specified by the Service Organization:    Control activities provide reasonable assurance that the annual plan valuation and underlying census data is accurately reported.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
11.11	<p>Individual employers selected for TRS allocation testing are asked to provide monthly payroll data from which a sample of employees is tested. Payroll data to be provided includes Employee Names, Payment Dates, Amount of Pay, Social Security Numbers, PID and Tier Status. Employees selected are tested on the following criteria:</p> <ul style="list-style-type: none"> <li>• Accuracy of age provided to RSA</li> <li>• Accuracy of gender provided to RSA</li> <li>• Accuracy of Retirement deductions made to RSA</li> </ul>	<p>Inspected the TRS allocation documentation provided by the Chief Financial Officer of RSA to determine that individual employers selected for TRS allocation testing were asked to provide monthly payroll data from which a sample of employees was tested and that payroll data to be provided included Employee Names, Payment Dates, Amount of Pay, Social Security Numbers, PID and Tier Status and that employees selected are tested on the following criteria:</p> <ul style="list-style-type: none"> <li>• Accuracy of age provided to RSA</li> <li>• Accuracy of gender provided to RSA</li> <li>• Accuracy of Retirement deductions made to RSA</li> </ul>	No exceptions noted.

**CONTROL AREA 12            INVESTMENT MANAGEMENT**

Control Objective Specified by the Service Organization:    Control activities provide reasonable assurance that investment activities are performed in accordance with the guidelines provided by the Board of Control and respective Investment Committee.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
12.1	Investment policies and procedures are in place to provide guidelines to the RSA employees responsible for executing investment transactions.	<p>Inquired of the Investment Accounting Manager regarding investment policies and procedures to determine that investment policies and procedures were in place to provide guidelines to the RSA employees responsible for executing investment transactions.</p> <p>Inspected the Investment Policy and Procedures documentation to determine that investment policies and procedures were in place to provide guidelines to the RSA employees responsible for executing investment transactions.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
12.2	Investment transactions are processed after completion in the order management system and upon receipt, signed trade tickets are reviewed for adherence to approved criteria and authorization by the CEO and respective Investment Committee Members.	<p>Inquired of the Investment Accounting Manager regarding the trade authorization and approval process to determine that investment transactions were processed after completion in the order management system and upon receipt, signed trade tickets were reviewed for adherence to approved criteria and authorization by the CEO and respective Investment Committee Members.</p> <p>Inspected a sample of investment transactions for a sample of days to determine that investment transactions were processed after completion in the order management system and upon receipt, signed trade tickets were reviewed for adherence to approved criteria and authorization by the CEO and respective Investment Committee Members.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

**CONTROL AREA 12            INVESTMENT MANAGEMENT**

Control Objective Specified by the Service Organization:    Control activities provide reasonable assurance that investment activities are performed in accordance with the guidelines provided by the Board of Control and respective Investment Committee.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
12.3	Monthly reconciliations are performed by Investment Accounting to help ensure that general ledger investment account balances are in agreement with the custodian of the funds and that investment activity had been posted to the correct accounts.	Inspected a sample of monthly reconciliations performed by Investment Accounting to determine that monthly reconciliations were performed by Investment Accounting to help ensure that general ledger investment account balances were in agreement with the custodian of the funds and that investment activity had been posted to the correct accounts.	No exceptions noted.