



A-LIGN



Public Education Employees'
Health Insurance Plan Type 2
SOC 1
2018



**REPORT ON MANAGEMENT'S DESCRIPTION OF PUBLIC EDUCATION
EMPLOYEES' HEALTH INSURANCE PLAN SYSTEM AND THE SUITABILITY OF
THE DESIGN
AND OPERATING EFFECTIVENESS OF CONTROLS**

**Pursuant to Statement on Standards for Attestation Engagements No. 18
(SSAE 18) Type 2**

October 1, 2017 through September 30, 2018

Table of Contents

| | |
|--|-----------|
| SECTION 1 INDEPENDENT SERVICE AUDITOR'S REPORT | 1 |
| SECTION 2 PUBLIC EDUCATION EMPLOYEES' HEALTH INSURANCE PLAN'S ASSERTION | 4 |
| SECTION 3 DESCRIPTION OF THE SYSTEM PROVIDED BY THE SERVICE ORGANIZATION | 7 |
| OVERVIEW OF OPERATIONS..... | 8 |
| Company Background | 8 |
| Description of Services Provided | 8 |
| CONTROL ENVIRONMENT | 18 |
| Integrity and Ethical Values | 18 |
| Commitment to Competence | 18 |
| Board of Directors Participation | 18 |
| Management's Philosophy and Operating Style..... | 19 |
| Organizational Structure and Assignment of Authority and Responsibility | 19 |
| Human Resources Policies and Practices | 19 |
| RISK ASSESSMENT | 20 |
| CONTROL OBJECTIVE AND RELATED CONTROL ACTIVITIES | 22 |
| MONITORING | 22 |
| INFORMATION AND COMMUNICATION SYSTEMS | 23 |
| Information Systems..... | 23 |
| Communication Systems | 25 |
| COMPLEMENTARY USER ENTITY CONTROLS..... | 25 |
| SECTION 4 TESTING OF CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES PROVIDED BY THE SERVICE AUDITOR..... | 27 |
| GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR | 28 |
| PHYSICAL SECURITY | 29 |
| NO EXCEPTIONS NOTED | 29 |
| ENVIRONMENTAL SAFEGUARDS | 31 |
| COMPUTER OPERATIONS - BACKUP | 34 |
| COMPUTER OPERATIONS - AVAILABILITY..... | 36 |
| DATA COMMUNICATION | 38 |
| INFORMATION SECURITY..... | 40 |
| CHANGE MANAGEMENT | 43 |
| ENROLLMENT | 44 |
| REVENUE - BILLING | 46 |
| REVENUE - COLLECTIONS | 50 |
| HEALTH INSURANCE BENEFITS | 55 |
| CLAIMS INCURRED BUT NOT REPORTED (IBNR)..... | 57 |
| INVESTMENT MANAGEMENT | 58 |

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT ON A DESCRIPTION OF THE PUBLIC EDUCATION EMPLOYEES' HEALTH INSURANCE PLAN'S SYSTEM AND THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS

To Public Education Employees' Health Insurance Plan:

We have examined the Public Education Employees' Health Insurance Plan's (PEEHIP) description of its Benefits Administration System at its Montgomery, Alabama locations for processing user entities' transactions for the period October 1, 2017 through September 30, 2018, and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description, based on the criteria identified in the "Public Education Employees' Health Insurance Plan Assertion" (assertion). 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 PEEHIP's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design and operating effectiveness of such complementary user entity controls.

PEEHIP uses Ventanex for credit card processing services, BBVA Compass Bank for ACH/EFT processing and banking services, Regions Bank for banking services, Blue Cross Blue Shield of Alabama (BCBS) for medical claims administration and flexible spending account services, MedImpact Healthcare Systems (MedImpact) for Core Pharmacy and Specialty Pharmacy claims administration services, Southland Benefit Solutions (Southland) for Cancer, Dental, Indemnity, and Vision claims administration services, United HealthCare (UHC) for Medicare Advantage claims administration services, VIVA Health (VIVA) for Hospital Medical claims administration services, LexisNexis for death notification services, Alabama Department of Public Health (ADPH) for death notification services, Segal Consulting for actuarial services, Bloomberg for financial software tools for analytics, equity trading, and data services, Eze Software Group (Eze) for trade order management services, Omgeo for U.S.-based financial markets trade allocation services, State Street Bank (State Street) for U.S.-based international holding company financial services, SimCorp for accounting and portfolio management solutions, and TradeWeb Markets (TradeWeb) for electronic over-the-counter marketplaces services. The description in Section 3 includes only the controls and related control objectives of PEEHIP and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by PEEHIP can be achieved only if complementary subservice organization controls assumed in the design of PEEHIP are suitably designed and operating effectively, along with the related controls at PEEHIP. Our examination did not extend to controls of the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

In Section 2 of this report, PEEHIP 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. PEEHIP 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, 2017 through September 30, 2018.

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 PEEHIP's assertion in Section 2 of this report,

- the description fairly presents the system that was designed and implemented for the period October 1, 2017 through September 30, 2018.
- 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, 2017 through September 30, 2018, and subservice organizations and user entities applied the complementary controls contemplated in the design of PEEHIP's controls for the period October 1, 2017 through September 30, 2018.
- the controls tested, which together with the complementary subservice organization and user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively for the period October 1, 2017 through September 30, 2018.

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 PEEHIP, user entities of PEEHIP's system during some or all of the period October 1, 2017 through September 30, 2018, 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-LIGN ASSURANCE

October 29, 2018
Tampa, Florida

SECTION 2

PUBLIC EDUCATION EMPLOYEES' HEALTH INSURANCE PLAN'S ASSERTION



Public Education Employees' Health Insurance Plan Assertion

October 29, 2018

We have prepared the description Public Education Employees' Health Insurance Plan's ("PEEHIP") Benefits Administration System for processing user entities' transactions during some or all of the period October 1, 2017, through September 30, 2018 (description) for user entities of the system during some or all of the period October 1, 2017, through September 30, 2018, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.


PEEHIP uses subservice organizations for credit card processing services, ACH/EFT processing, banking services, claims administration services, death notification services, actuarial services, investment trading and portfolio management services. The description includes only the control objectives and related controls of PEEHIP and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organizations' controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organizations.

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

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

- a. The description fairly presents the Public Education Employees' Health Insurance Plan ("PEEHIP") system made available to user entities of the system during some or all of the period October 1, 2017, through September 30, 2018, 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 Public Education Employees' Health Insurance Plan ("PEEHIP") 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 Public Education Employees' Health Insurance Plan ("PEEHIP") 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, 2017 through September 30, 2018 to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of PEEHIP's controls throughout the period October 1, 2017 through September 30, 2018. 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
Retirement Systems of Alabama

SECTION 3

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

OVERVIEW OF OPERATIONS

Company Background

The Public Education Employees' Health Insurance Plan (PEEHIP) was established in 1983 pursuant to the *Code of Alabama 1975, Title 16, Chapter 25A* (Act 455 of the Legislature of 1983) to provide a uniform plan of health insurance for active and retired employees of state and local educational institutions which provide instruction at any combination of grades K-14 (collectively, eligible employees), and to provide a method for funding the benefits related to the plan. The four-year universities participate in the plan with respect to their retired employees, and are eligible and may elect to participate in the plan with respect to their active employees. At this time, only two universities have elected to participate in the plan with respect to their active employees. Responsibility for the establishment of the health insurance plan and its general administration and operations is vested in the Public Education Employees' Health Insurance Board (Board). The Board is a corporate body for purposes of management of the health insurance plan. All assets of PEEHIP are held in trust for the payment of health insurance benefits. The Board has been appointed as the administrator of PEEHIP.

In order to comply with the reporting requirements set by GASB Statement No. 74, *Financial Reporting for Postemployment Benefit Plans Other Than Pension Plans*, the contributions and benefit payments related to retirees that are processed through PEEHIP are segregated from PEEHIP and reported as part of the Alabama Retired Education Employees' Health Care Trust (Trust). The Trust is a cost-sharing multiple-employer defined benefit postemployment healthcare plan that administers healthcare benefits to the retirees of participating state and local educational institutions. The Trust was established under the Alabama Retiree Health Care Funding Act of 2007 which authorized and directed Board to create an irrevocable trust to fund postemployment healthcare benefits to retirees. Active and retiree health insurance benefits are paid through PEEHIP. The assets of the Trust may not be used for any purpose other than to acquire permitted investments, pay administrative expenses, and provide postemployment healthcare benefits to or for retired employees and their dependents. The Alabama Legislature has no authority or power to appropriate the assets of the Trust. The Board periodically reviews the funds available in PEEHIP and determines if excess funds are available. If excess funds are determined to be available in PEEHIP, the Board authorizes a transfer of funds from PEEHIP to the Trust.

Description of Services Provided

Enrollment

The PEEHIP enrollment process is initiated when an employer enters a new eligible employee into the PEEHIP Employer Portal (Portal) on the Retirement Systems of Alabama's (RSA) website. Only new employees who meet the 'Guidelines for Insurance Eligibility' in the PEEHIP Member Handbook should be entered into the Portal. Every newly entered employee is mailed a New Member Packet with instructions for completing the enrollment process. They are also mailed a letter with their personal identification number (PID) and instructions for creating their account through the Member Online System (MOS) on RSA's website. Their MOS account must be created within 30 days of the employee's hire date as entered by their employer in the Portal. The PEEHIP Benefits Administration System (PBA System) business rules are configured in accordance with the eligibility guidelines in the PEEHIP Member Handbook to ensure that participant records are complete and to prevent ineligible employees from enrolling in PEEHIP.

Contributions

The *Code of Alabama 1975, Title 16, Chapter 25A, Articles 8 & 8.1* provide the Board with the authority to set the contribution requirements for plan participants and the employers for each required class, respectively. Additionally, the Board is required to certify to the Governor and the Legislature, the amount, as a monthly premium per active employee, necessary to fund the coverage of active and retired participant benefits for the following fiscal year. The Legislature then sets the premium rate per active employee in the annual appropriation bill.

For employees who retired after September 30, 2005, but before January 1, 2012, the employer contribution of the health insurance premium set forth by the Board for each retiree class is reduced by 2% for each year of service less than 25 and increased by 2% percent for each year of service over 25 subject to adjustment by the Board for changes in Medicare premium costs required to be paid by a retiree. In no case does the employer contribution of the health insurance premium exceed 100% of the total health insurance premium cost for the retiree.

For employees who retired after December 31, 2011, the employer contribution to the health insurance premium set forth by the Board for each retiree class is reduced by 4% for each year of service less than 25 and increased by 2% for each year over 25, subject to adjustment by the Board for changes in Medicare premium costs required to be paid by a retiree. In no case does the employer contribution of the health insurance premium exceed 100% of the total health insurance premium cost for the retiree. For employees who retired after December 31, 2011, who are not covered by Medicare, regardless of years of service, the employer contribution to the health insurance premium set forth by the Board for each retiree class is reduced by a percentage equal to 1% multiplied by the difference between the Medicare entitlement age and the age of the employee at the time of retirement as determined by the Board. This reduction in the employer contribution ceases upon notification to the Board of the attainment of Medicare coverage.

PEEHIP invoices both employers and participants monthly for the following month's premiums after the "all accounts pump" and full premium calculation is completed. This "pump" verifies the monthly premium amount for all active accounts to ensure that any and all account adjustments made since the previous month's invoicing cycle are reflected in the invoice amount. The invoices are generated in the PBA System which is the eligibility system that manages benefits eligibility for all PEEHIP participants and for all benefit plans offered. All invoices are reviewed and tested for accuracy by PEEHIP Accounting personnel. Any necessary corrections are made and the invoices are finalized. Once the invoices are generated, they are imported into the Great Plains (GP) Receivables Management System which is a subsidiary ledger used for PEEHIP accounts receivable management only. The invoices are imported into GP by participant account for future posting of payments and any accounts receivable follow up.

There are four types of invoices: employers, retirees, universities, and direct bills. Employer invoices include both the employer contributions and any out-of-pocket premiums owed by their employees who are also active PEEHIP participants. Employers access their finalized invoices through the Portal on PEEHIP's page on the RSA website. The retirees' invoice is billed to RSA for out-of-pocket premiums due from RSA retirees currently receiving a monthly retirement benefit payment. If a retiree's benefit payment is less than the amount owed to PEEHIP, they are listed on the exceptions report that accompanies the check, and the retiree is invoiced individually. Although they do not participate in PEEHIP as it relates to their active employees, Universities are invoiced for employer contributions for their retired employees who are PEEHIP participants. Their invoices are distributed via secure email. Direct bill invoices are for out-of-pocket premiums for coverage under COBRA or during a leave of absence from employment and those PEEHIP participants who are receiving a retirement benefit payment that is less than their PEEHIP premium. PEEHIP also direct bills both active and non-active participants for prescription drug claims paid after their coverage was cancelled. Direct bill invoices are mailed to the participants.

PEEHIP Accounting personnel review the Miscellaneous Unbilled Transactions Report on a monthly basis to determine whether premiums have been paid by all PEEHIP participants. This report captures unbilled transactions for all PEEHIP participants for a period of 4 to 5 months prior to the current month. Unbilled transactions occur as a result of a new employee's hire and coverage dates occurring between invoicing dates and is not included on the invoices generated by the PBA System. If an employee's hire and coverage dates are prior to the date on which the report is run, then an exception is noted and investigated. Once all exceptions have been resolved, the report is posted to GP and the appropriate parties are invoiced during the next invoice cycle.

Payments are processed daily when they are received. Payments by check are restrictively endorsed and deposited into the bank via the Remote Quick Deposit Program at Regions Bank. Any currency payments are sent to the bank by a bonded courier service. The entire day's payments are totaled and compared with the invoice reconciliations. The payments are batched into smaller groups and are compared to the sum of the individual invoice totals to ensure that the payments agree with the invoices. A cash receipt is created in STAARS to record the payments received on the general ledger. Then, the payments and invoice exceptions are posted in the subsidiary ledger through a lock-box process in GP. Any exceptions are reviewed and account adjustments are made, if necessary, to ensure that the payments are posted to the correct account. Any amounts still owed after the payments are processed through GP will be invoiced during the next cycle to the appropriate party.

PEEHIP also accepts payment by electronic check and credit card for those participants who receive direct bill invoices. Electronic payments are processed by Ventanex who settles and deposits the payments into an account at BBVA Compass. Each day, PEEHIP payments posted on Ventanex's website are reconciled with the settlements in the bank account. When this reconciliation is complete, the electronic payments are processed like the physical check payments.

On the 20th day of the month, pre-cancellation notices are mailed to those with unpaid invoices informing them that their payment must be postmarked no later than the last day of the month so as not to interrupt their coverage. Payments are reviewed daily through an automatic process for payments on claims hold accounts. A release file is sent to the carriers at the end of the day with accounts that can be released from claims hold. On the 3rd business day of the following month, coverage is cancelled if the payment has not been received.

Health Insurance Benefits

PEEHIP offers a basic hospital medical plan to active participants and non-Medicare eligible retirees. Benefits include inpatient hospitalization for a maximum of 365 days without a dollar limit, inpatient rehabilitation, outpatient care, physician services, and prescription drugs.

Active employees and non-Medicare eligible retirees who do not have Medicare eligible dependents can enroll in a health maintenance organization (HMO) in lieu of the basic hospital medical plan. The HMO includes hospital medical benefits, dental benefits, vision benefits, and an extensive formulary. However, participants in the HMO are required to receive care from a participating physician in the HMO plan.

PEEHIP offers four optional plans (Cancer, Dental, Hospital Indemnity, and Vision) that may be selected in addition to or in lieu of the basic hospital medical plan or MAPDP. The Hospital Indemnity Plan provides a per-day benefit for hospital confinement, maternity, intensive care, cancer, and convalescent care. The Cancer Plan covers cancer disease only and benefits are provided regardless of other insurance. Coverage includes a per-day benefit for each hospital confinement related to cancer. The Dental Plan covers diagnostic and preventive services, as well as basic and major dental services. Diagnostic and preventive services include oral examinations, teeth cleaning, x-rays, and emergency office visits. Basic and major services include fillings, general aesthetics, oral surgery not covered under a Group Medical Program, periodontics, endodontics, dentures, bridgework, and crowns. Dental services are subject to a maximum of \$1,250 per year for individual coverage and \$1,000 per person per year for family coverage. The Vision Plan covers annual eye examinations, eye glasses, and contact lens prescriptions.

PEEHIP participants may opt to elect the PEEHIP Supplemental Plan for hospital medical coverage in lieu of the PEEHIP Hospital Medical Plan. The PEEHIP Supplemental Plan provides secondary benefits to the participant's primary plan provided by another employer. Only active and non-Medicare retiree participants and dependents are eligible for the PEEHIP Supplemental Plan. There is no premium required for this plan, and the plan covers most out-of-pocket expenses not covered by the primary plan. The plan cannot be used as a supplement to Medicare, the PEEHIP Hospital Medical Plan, or the State and Local Government Plans administered by the State Employees' Insurance Board (SEIB).

PEEHIP remains primary for retirees until the retiree is Medicare eligible. If a participant or dependent is already Medicare eligible due to age or disability at the time of his or her retirement, Medicare will become the primary payer and PEEHIP the secondary payer effective on the date of the participant's retirement. A Medicare eligible retiree and/or Medicare eligible dependent must have both Medicare Part A (hospital insurance) and Part B (medical insurance) to have coverage with PEEHIP. Prior to January 1, 2017, all Medicare eligible participants and Medicare eligible covered dependents were automatically enrolled in the Medicare GenerationRx Medicare Part D Employer Group Waiver Program (EGWP) offered by PEEHIP unless already enrolled in a separate standard Medicare Part D plan or they choose not to participate or opt out.

Effective January 1, 2017, Medicare eligible participants and Medicare eligible dependents who are covered on a retiree contract were enrolled in the United HealthCare (UHC) Group Medicare Advantage plan for PEEHIP retirees. The MAPDP plan is fully insured by UHC and participants are able to have all of their Medicare Part A, Part B, and Part D (prescription drug coverage) in one convenient plan. With the UHC plan for PEEHIP, retirees can continue to see their same providers with no interruption and see any doctor who accepts Medicare on a national basis. Retirees have the same benefits in and out-of-network and there is no additional retiree cost share if a retiree uses an out-of-network provider and no balance billing from the provider.

PEEHIP employs a third-party administrator (TPA) to properly pay claims within the scope of the benefits determined by PEEHIP. Blue Cross Blue Shield of Alabama (BCBS) is the claims administrator for the hospital/medical, supplemental medical, and flexible spending account plans (Health Equity is a subcontractor of BCBS and administers the flexible spending plan). MedImpact Healthcare Systems, Inc., (MedImpact) is the claims administrator for the prescription drug plan. VIVA Health (VIVA) is the claims administrator for the HMO plan. Southland Benefit Solutions (Southland) is the claims administrator for the optional cancer, dental, indemnity, and vision plans. Medicare primary retired participants, their Medicare primary spouses/dependents on retired contracts, and Medicare primary surviving spouses are covered under a fully insured contract with UHC. An eligibility reconciliation is performed monthly to compare the carrier's participant data to PEEHIP's participant data. This reconciliation verifies that only eligible participants and their dependents are enrolled in PEEHIP in accordance with benefit provisions established and approved by the PEEHIP Board of Control.

Valuations

The actuary is provided the necessary census data files to complete the annual actuarial valuation for PEEHIP. The files that are provided to the actuary include eligible retirees and surviving spouses. All actuarial valuation data files sent to the actuaries are encrypted and protected by a password.

The retired file contains census data on existing eligible retired participants. The retired file includes PID, retirement type, age, gender, tobacco use, medical plan election, medical tier election, cancer coverage, dental coverage, indemnity coverage, vision coverage, spouse PID, spouse tobacco use, number of dependents, number of dependents taking medical coverage, and the number of dependents taking supplemental coverage. The census data in the retired files is tested for completeness and accuracy.

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

- Compare the number of records in the current year to the prior year
- Compare the number of service retirements in the current year to the prior year
- Compare the number of disability retirements in the current year to the prior year
- Compare the number of both male and female retirees in the current year to the prior year
- Compare the number of retirees with PPO/HMO coverage in the current year to the prior year
- Compare the number of retirees with supplemental coverage in the current year to the prior year
- Compare the number of retirees both using and not using tobacco in the current year to the prior year

- Compare the average age of retirees in the current year to the prior year
- Compare the number of dependents in the current year to the prior year
- Compare the number of dependents taking medical coverage in the current year to the prior year
- Compare the number of dependents taking optional coverage in the current year to the prior year

The surviving spouse file contains census data on existing eligible surviving spouses. The surviving spouse file includes PID, age, gender, tobacco use, medical plan election, medical tier election, cancer coverage, dental coverage, indemnity coverage, vision coverage, number of dependents, number of dependents taking medical coverage, and the number of dependents taking supplemental coverage. The census data in the surviving spouse files is tested for completeness and accuracy. Testing of the surviving spouse files includes, but is not limited to, the following:

- Compare the number of surviving spouses in the current year to the prior year
- Compare the number of surviving spouses both using and not using tobacco in the current year to the prior year
- Compare the number of dependents in the current year and prior year
- Compare the number of dependents taking medical coverage in the current year to the prior year
- Compare the number of dependents taking optional coverage in the current year to the prior year

The actuarial valuation files are checked for missing data such as date of birth, gender, and medical coverage to ensure the completeness of the census data. Any missing information that is identified is sent to the PEEHIP Benefits Division to obtain. The PEEHIP Benefits Division will then send the information back to the Accounting Division where an update query is run in Microsoft Access to update the necessary information in the valuation file. The PEEHIP Benefits Division also updates this information in the RSA DPAS and/or Legacy System.

All actuarial valuation data files are sent to the actuary upon approval by the Chief Financial Officer (CFO). Upon completion of the valuations, the actuaries provide preliminary results including a draft actuarial valuation report for PEEHIP. The draft copies are reviewed by Accounting personnel and the CFO.

Investment Management

The Board of Control invests and reinvests the funds of PEEHIP and the Trust 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.” The Trust is governed by its Investment Policy Statement within the Trust’s limitations and/or by other applicable legislative restrictions. Investment policies and procedures are in place to provide guidelines to the RSA employees responsible for executing investment transactions.

The Board Chair, on behalf of the full Board, grants the authority to purchase and sell securities on behalf of the Trust to the Secretary-Treasurer of the Board. Investment transactions are processed after completion in the trade order management system. Upon receipt, signed trade tickets are reviewed for adherence to approved criteria and proper authorization.

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

Significant Events

PEEHIP has implemented both 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 Health Insurance Plan. 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 to PEEHIP for the above services in each of the following functional areas:

| Division | Description |
|------------------------|--|
| Information Technology | The Information Technology ("IT") Division is responsible for activities associated with developing, maintaining, and supporting critical data processing systems. The organizational structure of the IT Division provides segregation of duties between client services, systems programming, application programming, computer operations, physical and logical security access, and documentation |
| PEEHIP Benefits | The PEEHIP Benefits Division is responsible for day-to-day benefit processing. This includes participant enrollment, account maintenance, and carrier reconciliations |
| Investments | The Investment Division is responsible for investing, executing, and reinvesting the funds of both PEEHIP and the Trust. This includes management of trades and investment positions |
| Accounting | The Accounting Division is responsible for receiving, identifying, posting, and depositing all contribution payments received each day accurately and timely. Monthly reconciliations are performed by Investment Accounting to ensure that general ledger investment account balances are in agreement with the balances reported by the custodian of the funds and that investment activity has been posted to the correct accounts. PEEHIP Accounting is also responsible for invoice reconciliations |

Boundaries of the System

The scope of this report includes the Public Education Employees' Health Insurance Plan ("PEEHIP") and the Alabama Retired Education Employees' Health Care Trust (Trust) which are both administered in the RSA Systems Building in Montgomery, Alabama.

Subservice Organizations

This report does not include the credit card processing services provided by Ventanex, the ACH/EFT processing and banking services provided by BBVA Compass Bank, the banking services provided by Regions Bank, the medical claims administration and flexible spending account services provided by Blue Cross and Blue Shield (BCBS), the Core Pharmacy and Specialty Pharmacy claims administration services provided by MedImpact, the Cancer, Dental, Indemnity, and Vision claims administration services provided by Southland, the Medicare Advantage claims administration services provided by United HealthCare (UHC), the Hospital Medical claims administration services provided by VIVA Health (VIVA), the death notification services provided by LexisNexis, the death notification services provided by Alabama Department of Public Health, the actuarial services provided by Segal Consulting, the financial software tools for analytics, equity trading, and data services provided by Bloomberg, the trade order management services provided by Eze Software Group, the U.S.-based financial markets trade allocation services provided by Omgeo, the U.S.-based international holding company financial services provided by State Street Bank, the accounting and portfolio management solutions provided by SimCorp, and the electronic over-the-counter marketplace services provided by TradeWeb Markets.

Subservice Organization Controls

PEEHIP's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called subservice organization controls. It is not feasible for all of the control objectives related to PEEHIP's services to be solely achieved by its control procedures. Accordingly, subservice organizations, in conjunction with their services, should establish their own internal controls or procedures to complement those of PEEHIP.

The following subservice organization controls should be implemented by Ventanex to provide additional assurance that the control objectives described within this report are met:

| Subservice Provider - Ventanex | |
|--------------------------------|---|
| Control Objective | Control |
| PEEHIP Revenue - Collections | Credit card payments are processed securely and in a timely manner by Ventanex |
| PEEHIP Revenue - Collections | Credit card payments are securely deposited into PEEHIP's bank account by Ventanex and PEEHIP is provided a list of payments that were received |

The following subservice organization controls should be implemented by BBVA Compass Bank to provide additional assurance that the control objectives described within this report are met:

| Subservice Provider - BBVA Compass Bank | |
|---|---|
| Control Objective | Control |
| PEEHIP Revenue - Collections | Secure ACH/EFT services for units and participants is provided by BBVA Compass Bank |
| PEEHIP Revenue - Collections | Securely processing ACH/EFT transactions, posting payments accurately to PEEHIP's bank account on a timely basis, and providing PEEHIP with an accurate and complete list of payments received is the responsibility of BBVA Compass Bank |

The following subservice organization controls should be implemented by Regions Bank to provide additional assurance that the control objectives described within this report are met:

| Subservice Provider - Regions Bank | |
|------------------------------------|---|
| Control Objective | Control |
| PEEHIP Revenue - Collections | Secure deposit terminals and applying deposits to PEEHIP's bank account accurately and timely is the responsibility of Regions Bank |

The following subservice organization controls should be implemented by BCBS to provide additional assurance that the control objectives described within this report are met:

| Subservice Provider - BCBS | |
|----------------------------|--|
| Control Objective | Control |
| PEEHIP Benefits | Claims are processed, adjudicated, and paid accurately and timely by BCBS |
| PEEHIP Benefits | A daily reconciliation of participants' information and coverage changes using the 834 files provided by PEEHIP is completed by BCBS |
| PEEHIP Benefits | PEEHIP is provided with full eligibility files on a monthly basis by BCBS |

| Subservice Provider - BCBS | |
|----------------------------|---|
| Control Objective | Control |
| PEEHIP Benefits | Rate schedules are defined by BCBS and PEEHIP is invoiced based on the rate schedules |

The following subservice organization controls should be implemented by MedImpact to provide additional assurance that the control objectives described within this report are met:

| Subservice Provider - MedImpact | |
|---------------------------------|---|
| Control Objective | Control |
| PEEHIP Benefits | Claims are processed, adjudicated, and paid accurately and timely by MedImpact |
| PEEHIP Benefits | A daily reconciliation of participants' information and coverage changes using the 834 files provided by PEEHIP is completed by MedImpact |
| PEEHIP Benefits | PEEHIP is provided with full eligibility files on a monthly basis by MedImpact |
| PEEHIP Benefits | Rate schedules are defined by MedImpact and PEEHIP is invoiced based on the rate schedules |

The following subservice organization controls should be implemented by Southland to provide additional assurance that the control objectives described within this report are met:

| Subservice Provider - Southland | |
|---------------------------------|---|
| Control Objective | Control |
| PEEHIP Benefits | Claims are processed, adjudicated, and paid accurately and timely by Southland |
| PEEHIP Benefits | A daily reconciliation of participants' information and coverage changes using the 834 files provided by PEEHIP is completed by Southland |
| PEEHIP Benefits | PEEHIP is provided with full eligibility files on a monthly basis by Southland |
| PEEHIP Benefits | Rate schedules are defined by Southland and PEEHIP is invoiced based on the rate schedules |

The following subservice organization controls should be implemented by UHC to provide additional assurance that the control objectives described within this report are met:

| Subservice Provider - UHC | |
|---------------------------|---|
| Control Objective | Control |
| PEEHIP Benefits | Claims are processed, adjudicated, and paid accurately and timely by UHC |
| PEEHIP Benefits | A daily reconciliation of participants' information and coverage changes using the 834 files provided by PEEHIP is completed by UHC |
| PEEHIP Benefits | PEEHIP is provided with full eligibility files on a monthly basis by UHC |
| PEEHIP Benefits | Rate schedules are defined by UHC and PEEHIP is invoiced based on the rate schedules |

The following subservice organization controls should be implemented by VIVA to provide additional assurance that the control objectives described within this report are met:

| Subservice Provider - VIVA | |
|-----------------------------------|--|
| Control Objective | Control |
| PEEHIP Benefits | Claims are processed, adjudicated, and paid accurately and timely by VIVA |
| PEEHIP Benefits | A daily reconciliation of participants' information and coverage changes using the 834 files provided by PEEHIP is completed by VIVA |
| PEEHIP Benefits | PEEHIP is provided with full eligibility files on a monthly basis by VIVA |
| PEEHIP Benefits | Rate schedules are defined by VIVA and PEEHIP is invoiced based on the rate schedules |

The following subservice organization controls should be implemented by LexisNexis to provide additional assurance that the control objectives described within this report are met:

| Subservice Provider - LexisNexis | |
|---|---|
| Control Objective | Control |
| PEEHIP Benefits | PEEHIP is notified of a decreased participant by LexisNexis in accordance with their contract |

The following subservice organization controls should be implemented by Alabama Department of Public Health to provide additional assurance that the control objectives described within this report are met:

| Subservice Provider - Alabama Department of Public Health | |
|--|--|
| Control Objective | Control |
| PEEHIP Benefits | PEEHIP is notified of a decreased participant by the Alabama Department of Public Health in accordance with their contract |

The following subservice organization controls should be implemented by Segal Consulting to provide additional assurance that the control objectives described within this report are met:

| Subservice Provider - Segal Consulting | |
|---|---|
| Control Objective | Control |
| PEEHIP Incurred but Not Reported (IBNR) | The IBNR (claims incurred by eligible participants but not yet reported) is calculated by Segal Consulting in accordance with the Claims Lag Triangle and enrollment counts |

The following subservice organization controls should be implemented by Bloomberg to provide additional assurance that the control objectives described within this report are met:

| Subservice Provider - Bloomberg | |
|--|--|
| Control Objective | Control |
| Investment Management | Real-time financial data, news feeds, and messages to facilitate the placement of trades are provided by Bloomberg |

The following subservice organization controls should be implemented by Eze Software Group to provide additional assurance that the control objectives described within this report are met:

| Subservice Provider - Eze Software Group | |
|---|--|
| Control Objective | Control |
| Investment Management | The trade data security and integrity in the trade order management system is maintained by Eze Software Group personnel |

The following subservice organization controls should be implemented by Omgeo to provide additional assurance that the control objectives described within this report are met:

| Subservice Provider - Omgeo | |
|------------------------------------|--|
| Control Objective | Control |
| Investment Management | Trade lifecycle events, including allocation, confirmation/affirmation, settlement notification, enrichment, operational analytics, and counterparty risk management between trade counterparties are automated by Omgeo |

The following subservice organization controls should be implemented by State Street Bank to provide additional assurance that the control objectives described within this report are met:

| Subservice Provider - State Street Bank | |
|--|--|
| Control Objective | Control |
| Investment Management | International holding company financial services are provided by State Street Bank |

The following subservice organization controls should be implemented by SimCorp to provide additional assurance that the control objectives described within this report are met:

| Subservice Provider - SimCorp | |
|--------------------------------------|---|
| Control Objective | Control |
| Investment Management | The investment accounting and portfolio management application for securities tracking, regulatory compliance, and report writing is provided and maintained by SimCorp |

The following subservice organization controls should be implemented by TradeWeb Markets to provide additional assurance that the control objectives described within this report are met:

| Subservice Provider - TradeWeb Markets | |
|---|--|
| Control Objective | Control |
| Investment Management | The security, integrity, and availability of the TradeWeb web platform is maintained by TradeWeb Markets |

PEEHIP management, along with the subservice provider, defines the scope and responsibility of the controls necessary to meet all the relevant control objectives through written contracts, such as service level agreements. In addition, PEEHIP monitors subservice organization controls through the following procedures:

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and subservice organization(s)
- Reviewing attestation reports over services provided by vendors and subservice organization(s)
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization

Significant Changes in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

CONTROL ENVIRONMENT

Integrity and Ethical Values

Management conveys integrity and ethical values to all levels of PEEHIP staff to help with performance and monitoring of business functions. PEEHIP 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 Teachers' Retirement System (TRS) statute, and to which PEEHIP would also be held, 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." All employees are subject to the ethics laws of the State of Alabama (*Code of Alabama 1975, Title 36, Chapter 25*) which prohibits any employee from using their 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 Interest with the Alabama Ethics Commission. RSA has an Investment Manual designed to assist Investment personnel 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 Human Resources' policies and procedures. Furthermore, the Department of Examiners of Public Accounts has the authority to perform a legal compliance audit of PEEHIP on a bi-annual basis.

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 to which employees are required to adhere
- Employees are required to 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

Management defines competency as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competency includes consideration of the competency levels for particular jobs and how those levels translate into the knowledge and skills required for a particular job.

Board of Directors Participation

Overall, the Board of Control coordinates their meetings and efforts with the personnel in the office of the Chief Executive Officer (CEO).

Corporate governance encompasses the internal policies and practices by which PEEHIP is operated and controlled on behalf of the State and its participants. The advantages of sound corporate governance include having a strong Board of Control that is accountable to the State, PEEHIP, and its participants. No member of the executive staff is a member of the governing board. The board consists of members elected by the membership or holding the board position because of their primary government position including the State Treasurer, the State Finance Director, and the State Superintendent of Education. The duties and responsibilities of the governing board are outlined in the statutes under which they were created.

At TRS's May 2017 meeting, the TRS Board voted in favor of quarterly meetings of both the TRS and PEEHIP Boards with special meetings held as the Board's business may require. All Board meetings are held with public notice filed with the Secretary of State in advance of the meeting with agendas and packages of information sent to members in advance of the meeting.

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

Management's Philosophy and Operating Style

To fully demonstrate the appropriate application of this principle, RSA and PEEHIP should display the following attributes: appropriate tone, influence over attitudes toward accounting principles and estimates, and an articulation of its objectives. Both RSA and PEEHIP believe 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 Risk |
| Articulates objectives | Risk Assessment |

Organizational Structure and Assignment of Authority and Responsibility

The organizational structure of RSA and PEEHIP provides the framework within which activities for achieving objectives are planned, executed, controlled, and monitored. The organizational structure described below details the divisions of the service organization that provide various services to all participating employers and participants. The structure provides for an adequate segregation of duties as well as clearly defined areas of responsibility.

Human Resources Policies and Practices

RSA and PEEHIP'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.

Human Resources (HR) carries out the policies and procedures mandated by the State Personnel Department. HR policy development for RSA and PEEHIP is performed by the HR Division that is operating at the corporate level. This group reviews, amends, or proposes new policies to include workplace behavior, compliance, 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 that policies require modification, the HR Division drafts the policy and reviews it with senior management. All policy changes must be approved by the CEO or Deputy Director.

Approved HR policies are documented and communicated to employees through various channels, including placement on the RSA intranet and verbally through senior management. RSA and PEEHIP employees are encouraged to review policies on a regular basis through the appropriate channels. Additionally, employees must agree to adhere to 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/or direct contact with HR. Policy violations normally result in disciplinary action ranging from oral reprimand to dismissal in accordance with the organization's policies and guidelines established under statute by the State Personnel Department.

PEEHIP complies with State Personnel procedures in hiring administrative personnel covered by the state merit system. For specific professional level personnel employed in unclassified positions, minimum criteria are established and applicants are screened through interviews and reference checks. When it is determined that a position needs to be filled, the hiring manager informs HR of the appropriate information related to the position. The HR Division 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 the appropriate personnel 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 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 be either a merit position within the state merit system or an unclassified position. If the position is within the merit system, the hiring manager will follow hiring rules established by the State Personnel Department and interview qualified candidates from the state's register for that job class. The hiring manager and HR interview qualified applicants, and a decision is made. If the position is outside of the merit system, it will be appropriately approved and the job description will be posted internally and on the RSA website. 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 the 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 policies and procedures related to employee conduct and information security in addition to specific job-related training.

RISK ASSESSMENT

RSA and PEEHIP maintain 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 are delineated in the enabling statutes and specifically include providing health insurance benefits to active and retired participants. Thus, the investment policies are the dominant aspect of planning and risk assessment. The Investment Division and Investment Advisor have quarterly economic update meetings in which they discuss asset allocations and the economic outlook for current and potential investments. PEEHIP 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 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 while taking into account both qualitative and quantitative materiality considerations.

Financial Reporting Risks

Management, specifically within the Accounting and Investment Divisions, 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 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 PEEHIP. The Investment Division meets with the Investment Advisor for an economic update quarterly to determine if any adjustments are needed in asset allocation within current authority. If modifications need to be made in the authorized allocation, then they would be presented to the full Board for approval. Legislative Counsel and Accounting personnel monitor legislative activity and advise the CEO and the Legislature of the potential impact of any proposed legislation.

The business process risk assessment is an 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 and/or preventing, the inherent risk of account and assertion, the volume of transactions, the history of errors, interaction with other controls, the competency of personnel, the complexity of the control, the level of automation, and the amount of change in the environment.

Fraud Risks

The Fraud Assessment focuses on the incentives, pressures, attitudes, rationalizations, and opportunities to commit fraud. The risk assessment is analyzed at two levels: first at the entity-wide level and then during the business process risk assessment during which controls are identified that mitigate the risk of fraud.

While PEEHIP 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.

PEEHIP 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 the State’s ethics laws in dealing with independent consultants and other third-party service providers.

To ensure the segregation of duties, cross-functional peer reviews of various reconciliations and specific risk areas have been implemented. For instance, Investment Accounting personnel does not reconcile their own work to balance to the global custodian.

CONTROL OBJECTIVE AND RELATED CONTROL ACTIVITIES

PEEHIP's control objectives and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the control objectives and related control activities are included in Section 4, they are, nevertheless, an integral part of PEEHIP's description of controls.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, adjacent to the service organization's description of controls. 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.

Integration with Risk Assessment

Along with assessing risks, PEEHIP 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 PEEHIP strives to achieve its business objectives. PEEHIP has applied a risk management approach to the organization in order to select and develop control activities. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed, and improved when necessary to meet the overall objectives of the organization.

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 PEEHIP.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in the Testing Matrices in addition 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, division of responsibilities, and weekly management meetings to discuss outstanding items and issues provides for real-time monitoring of operational activities in the Accounting Division. 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 and provides for hands-on monitoring.

Ongoing Monitoring

Management's close involvement in 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 based on whether the incident was isolated or requires a change in the organization's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of PEEHIP personnel.

Vendor Management

PEEHIP has defined the following activities to oversee controls performed by vendors that could impact the health insurance plan:

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and subservice organization(s)
- Reviewing attestation reports over services provided by vendors and subservice organization(s)
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization

Reporting Deficiencies

Internal tracking tools including reconciliations and trend reports are utilized to document and track the results of ongoing 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.

INFORMATION AND COMMUNICATION SYSTEMS

Information Systems

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

Infrastructure

Primary infrastructure used to conduct PEEHIP business 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 conduct PEEHIP business 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 |
| Library Manager | electronic filing application contains all correspondence sent and received related to RSA and PEEHIP participants and participating employers |
| Work Manager | workflow application that tracks all work items in the workflow environment |
| Customer Relationship Management (CRM) | tracking application through which RSA and PEEHIP staff documents all contact with their customers |
| My.StateStreet.com | Internet-based application which allows access to the RSA and PEEHIP's safekeeping accounts, including the ability to view, schedule, or download account information, activities, and statements |
| RSA Workbench System | Legacy system used to manage all accounts for those who participate in both RSA and PEEHIP |
| SimCorp Dimension | Investment accounting and portfolio management application for securities tracking, regulatory compliance, and report writing |
| STAARS | General ledger application used to record accounting transactions for RSA and PEEHIP |
| 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 |
| TradeSuite ID (Omgeo) | Application suite that offers automated 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

PEEHIP provides regular communication internally to employees and externally to participants, participating employers, business associates, etc. In developing internal communications, the appropriate managers work to determine the subject to be communicated and develop key message points to include. A wide array of communications are channeled to related parties of RSA and PEEHIP that include messages related to HR Policies, Executive Management Messages, Changes in the Operations, Mission, Vision, and/or Reporting or Compliance Requirements. A variety of communication channels are utilized to communicate internally, including meetings, when necessary. Communication with division personnel occurs primarily through e-mail. Similar to the division meetings, senior management meets as necessary. In addition to the meetings noted above, other communication channels utilized to communicate internally are e-mail, hardcopy publications, and face-to-face meetings. RSAConnect (RSA's intranet) is utilized to distribute key or critical information to employees.

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 between PEEHIP and its board members.

COMPLEMENTARY USER ENTITY CONTROLS

PEEHIP's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the control objectives related to PEEHIP's services to be solely achieved by PEEHIP control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of PEEHIP.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the control objectives described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

Control Objective 5 - Data Communication

1. Units are responsible for notifying PEEHIP of any errors when submitting files for processing.

Control Objective 6 - Information Security

2. Units and Participants are responsible for keeping user accounts and passwords confidential.

Control Objective 8 - Enrollment

3. Units are responsible for notifying PEEHIP of new employees who are eligible for health insurance benefits through PEEHIP in a timely manner.
4. Units and participants are responsible for providing complete and accurate participant enrollment information in a timely manner.
5. Units are responsible for notifying PEEHIP of terminated employees that are no longer eligible for PEEHIP benefits in a timely manner.
6. Units and participants are responsible for notifying PEEHIP if QLE's have occurred that allow for a change in coverage.

Control Objective 9 - PEEHIP Revenue - Billing

7. Units are responsible for reconciling employer invoices posted to the secure portal to the amount remitted from payroll deductions to PEEHIP.
8. Units are responsible for providing PEEHIP with a correction report for each invoicing cycle that identifies billings that the units believe are incorrect.
9. Units are responsible for ensuring that invoices are complete, accurate, and up-to-date.
10. Units and participants are responsible for notifying PEEHIP of any changes that relate to PEEHIP accounts and invoices that are handled by PEEHIP.
11. Units are responsible for notifying PEEHIP of changes made to technical or administrative contact information.

Control Objective 10 - PEEHIP Revenue - Collections

12. Units and participants are responsible for paying invoices in a timely manner.
13. Units are responsible for reconciling their monthly PEEHIP invoice to the dollar amount remitted to PEEHIP by providing the reconciling amounts by participant along with a reason for the reconciling item to PEEHIP.
14. Units and participants are responsible for reviewing invoices and notifying PEEHIP of any discrepancies.
15. Units and participants are responsible for notifying PEEHIP of any changes that relate to PEEHIP account information.
16. Units and participants are responsible for opening and responding to mail received from PEEHIP on a timely basis.

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 ASSURANCE's examination of the controls of PEEHIP was limited to the control objectives and related control activities specified by the management of PEEHIP and did not encompass all aspects of PEEHIP'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. 18 (SSAE 18).

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

| TEST | DESCRIPTION |
|----------------|--|
| 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 18 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 access control policies and guidelines 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. 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 retained video footage 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 th 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 th floor. Inspected the data center 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 |
|---------------|---|---|----------------------|
| 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 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. |
| 1.6 | The facilities are protected with a centralized panic alarm system that is monitored by a 24/7 alarm monitoring company. | 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. |
| 1.7 | 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. | 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. 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. | No exceptions noted. No exceptions noted. |
| 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 once every two weeks 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 once every two weeks 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.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---------------|--|--|--|
| 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 server room humidity monitoring and water detection system 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. Inspected the data center humidity and water detection monitoring application 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. 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. |
| 2.9 | An uninterruptable power supply (UPS) is in place to provide power to critical infrastructure equipment in the event of a temporary power loss or power surge. | Observed the UPS systems to determine that an uninterruptable power supply (UPS) was in place to provide power to critical infrastructure equipment in the event of a temporary power loss or power surge. | No exceptions noted. |
| 2.10 | The UPS units are inspected and maintained by a third party on an annual basis. | Inspected the most recent UPS inspection and maintenance report to determine that the UPS units were inspected and maintained by a third party on an annual basis. | 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 |
|---------------|--|--|----------------------|
| 2.11 | The UPS units are configured to monitor the UPS batteries and notify appropriate personnel if battery conditions change. | Inspected the UPS configurations and an example battery alert to determine that the UPS units were configured to monitor the UPS batteries and notify appropriate personnel if battery conditions changed. | No exceptions noted. |
| 2.12 | The UPS units are configured to monitor and alert personnel of changing UPS power conditions. | Inspected the UPS configurations and an example alert to determine that the UPS units were configured to monitor and alert personnel of changing UPS power conditions. | 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. | Inquired of the Security & 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. | No exceptions noted. |
| | | 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. | 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 |
|---------------|---|---|----------------------|
| 3.5 | 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 data center and the data center in Mobile. | Inspected the replication configurations and replication logs for a sample of days to determine that RSA used Data Domain and EMC Avamar devices that provided deduplication between the main 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 procedures 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. | Observed the incident ticket management system to determine that an incident ticket management system was in place to assign, track, and monitor operational incidents. | No exceptions noted. |
| | | Inspected operational incident tickets for a sample of incidents 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, internal scripts and an example notification 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. |

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 |
|---------------|--|--|----------------------|
| 4.5 | 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 once 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 once per week. | No exceptions noted. |
| 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. | Inquired of the Security & 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. 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. | No exceptions noted. No exceptions noted. |
| 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. | Inquired of the Security & 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. Inspected the firewall administrator access listing to determine that management restricted the ability to administer the firewall system to the appropriate IT personnel. | No exceptions noted. No exceptions noted. |
| 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. | Inspected the virtual private network (VPN) configuration, log in screen, 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. Inquired of the Security & 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. | No exceptions noted. No exceptions noted. |
| 5.6 | The firewall system requires administrators to authenticate via an authorized user account and password prior to performing administration tasks. | Inspected the firewall system configurations to determine that the firewall system was configured to deny general access and permit access based on IP address. Inquired of the Security & 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. 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. | No exceptions noted. 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 |
|---------------|--|---|--|
| 6.1 | 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. Inspected the listing of administrators on the network domain to determine that administrator access within the network domain was restricted to authorized individuals. | No exceptions noted. No exceptions noted. |
| 6.3 | 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: <ul style="list-style-type: none">• Enforce password history• Maximum password age• Minimum password length• Password must meet complexity requirements• Account lockout | 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: <ul style="list-style-type: none">• Enforce password history• Maximum password age• Minimum password length• Password must meet complexity requirements• Account lockout | 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 | 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: <ul style="list-style-type: none">• Enforce password history• Maximum password age• Minimum password length• Password must meet complexity requirements | 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: <ul style="list-style-type: none">• Enforce password history• Maximum password age• Minimum password length• Password must meet complexity requirements | 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. |
| 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. |

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 |
|---------------|--|--|---|
| 6.9 | User accounts are assigned to predefined access roles to restrict access to certain functions within the applications. | <p>Inquired of the Security & 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 | Policies and procedures are in place to guide PEEHIP personnel, employers, and participants on their responsibilities regarding participant enrollment. | Inspected the PEEHIP participant enrollment policies and procedures document to determine that policies and procedures were in place to guide PEEHIP personnel, employers, and participants on their responsibilities regarding participant enrollment. | No exceptions noted. |
| 8.2 | During initial enrollment, the PEEHIP Benefits Administration System (PBASystem) is configured to prevent non-eligible employees from being added as participants and ensures participant records are complete. | Inquired of the CFO regarding the PBA System configurations to determine that during initial enrollment, the PBA System was configured to prevent non-eligible employees from being added as participants and ensures participant records were complete. | No exceptions noted. |
| | | Inspected the PBA System configurations to determine that during initial enrollment, the PBA System was configured to prevent non-eligible employees from being added as participants and ensures participant records were complete. | No exceptions noted. |
| 8.3 | The PBA System is configured to automatically prevent participant enrollment after 30 days of an employee's hire date. | Inquired of the CFO regarding the PBA System enrollment date configurations to determine that the PBA System was configured to automatically prevent participant enrollment after 30 days of an employee's hire date. | No exceptions noted. |
| | | Inspected the PBA System enrollment configurations to determine that the PBA System was configured to automatically prevent participant enrollment after 30 days of an employee's hire date. | 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 |
|---------------|--|---|---|
| 8.4 | The PBA System is configured to only allow participants to change coverage if a qualifying life event (QLE) occurs or during the open enrollment period. | <p>Inquired of the CFO regarding the PBA System coverage change configurations to determine that the PBA System was configured to only allow participants to change coverage if a qualifying life event (QLE) occurred or during the open enrollment period.</p> <p>Inspected the PBA System coverage change configurations to determine that the PBA System was configured to only allow participants to change coverage if a qualifying life event (QLE) occurred or during the open enrollment period.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

CONTROL AREA 9**REVENUE - BILLING**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that members are billed in accordance with their account type for the correct amount based upon rate schedules approved by the PEEHIP Board of Control.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---------------|---|--|----------------------|
| 9.1 | Policies and procedures are in place to guide PEEHIP personnel in the revenue billing processes. | Inspected the PEEHIP revenue policies and procedures documents to determine that policies and procedures were in place to guide PEEHIP personnel in the revenue billing processes. | No exceptions noted. |
| 9.2 | Units' contributions and participants' premiums for both active and retired participants and all copay and deductible requirements are approved by the PEEHIP Board of Control. | Inspected PEEHIP Board of Control's approval for units' contributions and members premiums for active and retired members and all copay and deductible requirements to determine that units' contributions and participants' premiums for both active and retired participants and all copay and deductible requirements were approved by the PEEHIP Board of Control. | No exceptions noted. |
| 9.3 | The PBA System uses business rules from the PEEHIP Member Handbook to automatically identify eligibility, coverage, and premiums for each participant. | Inspected the PEEHIP member handbook and PEEHIP new rates table to determine that the PBA System used business rules from the PEEHIP Member Handbook to automatically identify eligibility, coverage, and premiums for each participant. | No exceptions noted. |
| 9.4 | PEEHIP revenue schedules are created monthly by the Director of Revenue and indicates the invoicing cycle dates for the month. | Inspected PEEHIP revenue schedules for a sample of months to determine that PEEHIP revenue schedules were created monthly by the Director of Revenue and indicated the invoicing cycle dates for the month. | No exceptions noted. |

CONTROL AREA 9**REVENUE - BILLING**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that members are billed in accordance with their account type for the correct amount based upon rate schedules approved by the PEEHIP Board of Control.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---------------|---|---|----------------------|
| | Invoicing Cycle - Employers | | |
| 9.5 | The PBA System is configured to perform a monthly "all accounts pump" and full premium calculation on the first Saturday of each month. The "all accounts pump" calculates the premiums for all accounts that will be billed during the next invoicing cycle. | Inspected the PBA System monthly all accounts pump configurations and the all accounts pump report for a sample of months to determine that the PBA System was configured to perform a monthly "all accounts pump" and full premium calculation on the first Saturday of each month, and that the "all accounts pump" calculated the premiums for all accounts that will be billed during the next invoicing cycle. | No exceptions noted. |
| 9.6 | Invoices for employer contributions and out-of-pocket premiums due for active participants are tested and reviewed by a PEEHIP Accountant on a monthly basis for completeness and accuracy. Corrections to the invoices are made, if necessary. | Inspected employer contributions and out-of-pocket premiums testing and review for a sample of months to determine that invoices for employer contributions and out-of-pocket premiums due for active participants were tested and reviewed by a PEEHIP Accountant on a monthly basis for completeness and accuracy, and that corrections to the invoices were made, if necessary. | No exceptions noted. |
| 9.7 | Finalized employer invoices are distributed via secure portal to the employers. | Inspected the secure employer portal website and email confirmation of employer invoices being uploaded for a sample of months to determine that finalized employer invoices were distributed via secure portal to the employers. | No exceptions noted. |
| | Invoicing Cycle - Retirees | | |
| 9.8 | Invoices for retired participants are tested and reviewed by a PEEHIP Accountant on a monthly basis for completeness and accuracy. Corrections to the invoice are made, if necessary. | Inspected retired members invoice review and testing for a sample of months to determine that invoices for retired participants were tested and reviewed by a PEEHIP Accountant on a monthly basis for completeness and accuracy, and that corrections to the invoice were made, if necessary. | No exceptions noted. |

CONTROL AREA 9**REVENUE - BILLING**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that members are billed in accordance with their account type for the correct amount based upon rate schedules approved by the PEEHIP Board of Control.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------------------------------------|---|--|---|
| 9.9 | A retirees' exception report is provided by the Member Payroll Accounting Division on a monthly basis for premiums that will not be deducted from retirement benefit payments being issued to a retiree. These premiums are reviewed for adjustments or future direct billings to retirees. | <p>Inquired of the Assistant Chief Financial Officer regarding the retirees' exception report to determine that a retirees' exception report was provided by the Member Payroll Accounting Division on a monthly basis for premiums that would not be deducted from retirement benefit payments being issued to a retiree, and that these premiums were reviewed for adjustments or future direct billings to retirees.</p> <p>Inspected the retirees' exception report and the retirees' exception report review for a sample of months to determine that a retirees' exception report was provided by the Member Payroll Accounting Division on a monthly basis for premiums that would not be deducted from retirement benefit payments being issued to a retiree, and that these premiums were reviewed for adjustments or future direct billings to retirees.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> |
| Invoicing Cycle - University | | | |
| 9.10 | University invoices are tested and reviewed by a PEEHIP Accountant on a monthly basis for completeness and accuracy. Corrections to the invoices are made, if necessary. | Inspected university retirees' invoice testing and review for a sample of months to determine that university invoices were tested and reviewed by a PEEHIP Accountant on a monthly basis for completeness and accuracy, and that corrections to the invoices were made, if necessary. | No exceptions noted. |
| 9.11 | Finalized invoices for university employer contributions are distributed via secure email to the Universities. | Inspected secure emails to the Universities containing finalized invoices for a sample of months to determine that finalized invoices for university employer contributions were distributed via secure email to the Universities. | No exceptions noted. |

CONTROL AREA 9**REVENUE - BILLING**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that members are billed in accordance with their account type for the correct amount based upon rate schedules approved by the PEEHIP Board of Control.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---------------|--|--|----------------------|
| | Invoicing Cycle - Direct Bill | | |
| 9.12 | Direct bill invoices are tested and reviewed by a PEEHIP Accountant on a monthly basis for completeness and accuracy. Corrections to the invoices are made, if necessary. | Inspected direct bill invoice testing and review for a sample of months to determine that direct bill invoices were tested and reviewed by a PEEHIP Accountant on a monthly basis for completeness and accuracy, and that corrections to the invoices were made, if necessary. | No exceptions noted. |
| 9.13 | On a monthly basis, PEEHIP will bill both active and non-active participants upon notification from MedImpact of prescription claims paid after a cancellation date. A PEEHIP Accountant reviews the bills for accuracy. | Inspected billing records and active and non-active bill review for a sample of months to determine that on a monthly basis, PEEHIP billed both active and non-active participants upon notification from MedImpact of prescription claims paid after a cancellation date, and that a PEEHIP Accountant reviewed the bills for accuracy. | No exceptions noted. |
| | Invoicing Cycle - Miscellaneous Unbilled Transactions | | |
| 9.14 | An unbilled transactions report is produced routinely during the month by a PEEHIP Accountant. The report captures any unbilled transactions for 4 to 5 months prior to the current month which have not been invoiced through the PBA System. | Inspected the unbilled transaction report for a sample of months to determine that an unbilled transactions report was produced routinely during the month by a PEEHIP Accountant, and that the report captured any unbilled transactions for 4 to 5 months prior to the current month which had not been invoiced through the PBA System. | No exceptions noted. |
| 9.15 | The PEEHIP Accountant reviews the unbilled transactions report and researches any unbilled transactions on a monthly basis. Corrections are made, if necessary. | Inspected the unbilled transaction report and unbilled transaction report review for a sample of months to determine that the PEEHIP Accountant reviewed the unbilled transactions report and researched any unbilled transactions on a monthly basis, and that corrections were made, if necessary. | No exceptions noted. |

CONTROL AREA 10**REVENUE - COLLECTIONS**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that invoices are collected, cash is deposited timely and any unpaid accounts are worked in accordance with PEEHIP policy.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--------------------------------|---|--|----------------------|
| 10.1 | Policies and procedures are in place to guide PEEHIP personnel in the revenue collection processes. | Inspected the PEEHIP revenue collection policies and procedures document to determine that policies and procedures were in place to guide PEEHIP personnel in the revenue collection processes. | No exceptions noted. |
| 10.2 | Each participant is assigned an 8-digit customer numeric number. The number is used to ensure payments are posted to the correct account. | Inspected the customer numeric number for a sample of members to determine that each participant was assigned an 8-digit customer numeric number, and that the number was used to ensure payments were posted to the correct account. | No exceptions noted. |
| Collections - Employers | | | |
| 10.3 | Employer contribution payments are reconciled to the employer invoices on a monthly basis as the payments are received. | Inspected employer invoice totals and collection reconciliations for a sample of employer payments to determine that employer contribution payments were reconciled to the employer invoices on a monthly basis as the payments were received. | No exceptions noted. |
| 10.4 | Employer contribution payments are deposited into the bank upon receipt. | Inspected deposit statements for a sample of employer payments to determine that employer contribution payments were deposited into the bank upon receipt. | No exceptions noted. |

CONTROL AREA 10**REVENUE - COLLECTIONS**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that invoices are collected, cash is deposited timely and any unpaid accounts are worked in accordance with PEEHIP policy.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------------------------------|--|---|--|
| 10.5 | Segregation of duties exist during the employer contributions collection process. Different Accounting personnel perform the following tasks: <ul style="list-style-type: none"> • Open mail and endorse checks • Batch payments and reconcile batches to the corresponding employer invoices • Verify the payment totals and deposit payments into the bank • Process the payments and invoice exceptions | Observed the employer contributions process to determine that segregation of duties existed during the employer contributions collection process, and that different Accounting personnel performed the following tasks: <ul style="list-style-type: none"> • Opened mail and endorsed checks • Batched payments and reconciled batches to the corresponding employer invoices • Verified the payment totals and deposited payments into the bank • Processed the payments and invoiced exceptions | No exceptions noted. |
| 10.6 | On a monthly basis, unpaid employer contributions are invoiced as premiums and mailed to the corresponding employer. | Inspected direct bill premium invoices for a sample of direct bill participates to determine that on a monthly basis, unpaid employer contributions were invoiced as premiums and mailed to the corresponding employer. | No exceptions noted. |
| Collections - Retirees | | | |
| 10.7 | The payroll deduction check for retiree premiums is hand delivered to the Revenue Accounting Division by Member Payroll Accounting personnel on a monthly basis. | Inquired of the Assistant Chief Financial Officer regarding the retirees' payroll deduction check to determine that the payroll deduction check for retiree premiums was hand delivered to the Revenue Accounting Division by Member Payroll Accounting personnel on a monthly basis. Inspected the PEEHIP revenue collection policies and procedures document to determine that the payroll deduction check for retiree premiums was hand delivered to the Revenue Accounting Division by Member Payroll Accounting personnel on a monthly basis. | No exceptions noted. No exceptions noted. |

CONTROL AREA 10**REVENUE - COLLECTIONS**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that invoices are collected, cash is deposited timely and any unpaid accounts are worked in accordance with PEEHIP policy.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---------------|---|--|----------------------|
| 10.8 | The payroll deduction check for retiree premiums is reviewed and reconciled to the corresponding invoice on a monthly basis by a PEEHIP accountant. | Inspected retirees' invoice totals and collection reconciliations for a sample of retirees' payments to determine that the payroll deduction check for retiree premiums was reviewed and reconciled to the corresponding invoice on a monthly basis by a PEEHIP accountant. | No exceptions noted. |
| 10.9 | The payroll deduction check for retiree premiums is deposited into the bank each month upon receipt. | Inspected deposit statements for a sample of retirees' payments to determine that the payroll deduction check for retiree premiums was deposited into the bank each month upon receipt. | No exceptions noted. |
| 10.10 | On a monthly basis, unpaid retirees' premiums that are not covered by their retirement checks are invoiced and mailed to the corresponding participants. | Inspected direct bill premium invoices for a sample of direct bill participants to determine that on a monthly basis, unpaid retirees' premiums that were not covered by their retirement checks were invoiced and mailed to the corresponding participants. | No exceptions noted. |
| 10.11 | Segregation of duties exist during the retirees' premiums collection process. Different accounting personnel perform the following tasks: <ul style="list-style-type: none">• Endorse retiree premium checks• Deposit retiree checks into the bank• Process the payment | Observed the retirees' premiums collection process to determine that segregation of duties existed during the retirees' premiums collection process, and that different accounting personnel performed the following tasks: <ul style="list-style-type: none">• Endorsed retiree premium checks• Deposited retiree checks into the bank• Processed the payment | No exceptions noted. |
| | Collections - University | | |
| 10.12 | University employer contributions are reconciled to the university employer invoices on a monthly basis as the payments are received. | Inspected university invoice totals and collection reconciliations for a sample of university payments to determine that university employer contributions were reconciled to the university employer invoices on a monthly basis as the payments were received. | No exceptions noted. |

CONTROL AREA 10**REVENUE - COLLECTIONS**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that invoices are collected, cash is deposited timely and any unpaid accounts are worked in accordance with PEEHIP policy.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---------------|---|--|----------------------|
| 10.13 | University employer contribution payments are deposited into the bank upon receipt. | Inspected deposit statements for a sample of university payments to determine that university employer contribution payments were deposited into the bank upon receipt. | No exceptions noted. |
| 10.14 | Segregation of duties exist during the university contributions collection process. Different accounting personnel perform the following tasks: <ul style="list-style-type: none">• Open mail, endorse checks, and reconcile ACH/wire and check contribution payments to the corresponding invoices• Batch payments and reconcile batches to the universities' invoices• Verify the payment totals and deposit payments into the bank• Process the payments and invoice exceptions | Observed the universities premiums collection process to determine that segregation of duties existed during the university contributions collection process, and that different accounting personnel performed the following tasks: <ul style="list-style-type: none">• Opened mail, endorsed checks, and reconciled ACH/wire and check contribution payments to the corresponding invoices• Batched payments and reconciled batches to the universities' invoices• Verified the payment totals and deposited payments into the bank• Processed the payments and invoiced exceptions | No exceptions noted. |
| 10.15 | On a monthly basis, unpaid employer contributions are invoiced and mailed to the corresponding employers. | Inspected direct bill premium invoices for a sample of direct bill participates to determine that on a monthly basis, unpaid employer contributions were invoiced and mailed to the corresponding employers. | No exceptions noted. |
| | Collections - Direct Bills | | |
| 10.16 | Direct bill premium payments are reconciled to direct bill invoices upon receipt of payment. | Inspected direct bill invoice totals and collection reconciliations for a sample of direct bill payments to determine that direct bill premium payments were reconciled to direct bill invoices upon receipt of payment. | No exceptions noted. |

CONTROL AREA 10**REVENUE - COLLECTIONS**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that invoices are collected, cash is deposited timely and any unpaid accounts are worked in accordance with PEEHIP policy.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---------------|--|---|----------------------|
| 10.17 | Direct bill premium payments are deposited into the bank upon receipt of payment. | Inspected deposit statements for a sample of direct bill payments to determine that direct bill premium payments were deposited into the bank upon receipt of payment. | No exceptions noted. |
| 10.18 | A pre-cancellation notice is sent around the 20 th day of the month to participants that have not remitted payment for unpaid invoices. The notice advises the participant that payment must be postmarked by the last day of the month to avoid interrupting their coverage. | Inspected pre-cancellation notices for a sample of direct bill payments to determine that a pre-cancellation notice was sent around the 20 th day of the month to participants that had not remitted payment for unpaid invoices, and that the notice advised the participant that payment must be postmarked by the last day of the month to avoid interrupting their coverage. | No exceptions noted. |
| 10.19 | Past due premiums are investigated, and changes are made to invoices, if necessary, as premiums become past due. | Inspected past due premiums investigations and premium changes for a sample of direct bill payments to determine that past due premiums were investigated, and changes were made to invoices, if necessary, as premiums became past due. | No exceptions noted. |
| 10.20 | Participants' coverage is cancelled if premiums have not been paid by the 3 rd business day of the following month. | Inspected participants' cancellation notice for a sample of direct bill payments to determine that participants' coverage was cancelled if premiums had not been paid by the 3 rd business day of the following month. | No exceptions noted. |

CONTROL AREA 11**HEALTH INSURANCE BENEFITS**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that benefits are paid accurately and timely for eligible members and dependents.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---------------|---|---|----------------------|
| 11.1 | Documented policies and procedures are in place to guide PEEHIP personnel through the benefits process. | Inspected the PEEHIP benefits policies and procedures document and the member handbook to determine that documented policies and procedures were in place to guide PEEHIP personnel through the benefits process. | No exceptions noted. |
| 11.2 | Third party carriers' attestation reports (SOC 2 reports) are obtained and evaluated on an annual basis. | Inspected the third party carrier's attestation reports and evaluations to determine that third party carriers' attestation reports (SOC 2 reports) were obtained and evaluated on an annual basis. | No exceptions noted. |
| 11.3 | Claims' payments are reviewed and approved by the CFO on a monthly basis. | Inspected claim payment approvals for a sample of months to determine that claims' payments were reviewed and approved by the CFO on a monthly basis. | No exceptions noted. |
| 11.4 | On a monthly basis, accounting personnel perform detailed reconciliations and examinations of claims data to validate the accuracy and completeness of participant records and information. | Inspected detailed reconciliations of all carrier's invoices for a sample of months to determine that on a monthly basis, accounting personnel performed detailed reconciliations and examinations of claims data to validate the accuracy and completeness of participant records and information. | No exceptions noted. |
| 11.5 | 834 files noting changes to participant information and coverage are provided to the carriers on a daily basis. | Inspected 834 files for a sample of days and emails indicating that the files were sent to the carriers to determine that 834 files noting changes to participant information and coverage were provided to the carriers on a daily basis. | No exceptions noted. |
| 11.6 | PEEHIP verifies participant eligibility by reconciling PEEHIP's records to carriers' records on a monthly basis. Any discrepancies are reviewed and resolved in a timely manner. | Inspected the full eligibility reconciliations for a sample of months to determine that PEEHIP verified participant eligibility by reconciling PEEHIP's records to carriers' records on a monthly basis, and that any discrepancies were reviewed and resolved in a timely manner. | No exceptions noted. |

CONTROL AREA 11**HEALTH INSURANCE BENEFITS**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that benefits are paid accurately and timely for eligible members and dependents.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---------------|---|--|---|
| 11.7 | PEEHIP is notified of a participant's death when the date of death is entered in the Person Tool within the RSA Workbench System. This update triggers an automated process through which coverage is cancelled to ensure payments are not made for the benefits of a deceased participant. | <p>Inquired of the Chief Financial Officer regarding notification of participant's death to determine that PEEHIP was notified of a participant's death when the date of death was entered in the Person Tool within the RSA Workbench System, and that this update triggered an automated process through which coverage was cancelled to ensure payments were not made for the benefits of a deceased participant.</p> <p>Inspected the automated computer death notification services contract and the most recent notification to determine that PEEHIP was notified of a participant's death when the date of death was entered in the Person Tool within the RSA Workbench System, and that this update triggered an automated process through which coverage was cancelled to ensure payments were not made for the benefits of a deceased participant.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

CONTROL AREA 12**CLAIMS INCURRED BUT NOT REPORTED (IBNR)**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that the incurred but not reported PEEHIP liability at the end of the year is fairly stated.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---------------|---|--|----------------------|
| 12.1 | The CFO and a Financial Analyst prepare a Claims Lag Triangle at the end of each fiscal year by compiling historical claims data. | Inquired of the CFO regarding the Claims Lag Triangle to determine that the CFO and a Financial Analyst prepared a Claims Lag Triangle at the end of each fiscal year by compiling historical claims data. | No exceptions noted. |
| | | Inspected the most recent Claims Lag Triangle calculations to determine that the CFO and a Financial Analyst prepared a Claims Lag Triangle at the end of each fiscal year by compiling historical claims data. | No exceptions noted. |
| 12.2 | PEEHIP submits the Claims Lag Triangle and enrollment counts to the actuary to calculate IBNR (claims incurred by eligible participants but not yet reported). The calculated IBNR is recorded and reported on the year-end financial statements. | Inquired of the CFO regarding the process of calculating the IBNR to determine that PEEHIP submitted the Claims Lag Triangle and enrollment counts to the actuary to calculate IBNR (claims incurred by eligible participants but not yet reported), and that the calculated IBNR was recorded and reported on the year-end financial statements. | No exceptions noted. |
| | | Inspected the most recent Claims Lag Triangle calculations, actuarial reserve study report and year-end financial statements to determine that PEEHIP submitted the Claims Lag Triangle and enrollment counts to the actuary to calculate IBNR (claims incurred by eligible participants but not yet reported), and that the calculated IBNR was recorded and reported on the year-end financial statements. | No exceptions noted. |

CONTROL AREA 13 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 |
|---------------|---|--|----------------------|
| 13.1 | Investment policies and procedures are in place to provide guidelines to the employees responsible for executing investment transactions. | 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 employees responsible for executing investment transactions. | No exceptions noted. |
| | | Inspected the investment policy and procedures documentation to determine that investment policies and procedures were in place to provide guidelines to the employees responsible for executing investment transactions. | No exceptions noted. |
| 13.2 | 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 proper authorization. | 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 proper authorization. | No exceptions noted. |
| | | Inspected 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 proper authorization. | No exceptions noted. |

CONTROL AREA 13 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 |
|---------------|--|--|----------------------|
| 13.3 | 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 has been posted to the correct accounts. | Inspected monthly reconciliations performed by Investment Accounting for a sample of months 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 has been posted to the correct accounts. | No exceptions noted. |