



A-LIGN



MidAmerica Administrative &  
Retirement Solutions, Inc.  
Type 2 SSAE 16  
2015



**REPORT ON MANAGEMENT'S DESCRIPTION OF MIDAMERICA ADMINISTRATIVE  
& RETIREMENT SOLUTIONS, INC.'S SYSTEM AND ASPECTS OF COMPUTER  
DATA NETWORKS' SYSTEM AND THE SUITABILITY OF THE DESIGN AND  
OPERATING EFFECTIVENESS OF CONTROLS**

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

**October 1, 2014 Through September 30, 2015**

## Table of Contents

<b>SECTION 1 INDEPENDENT SERVICE AUDITOR’S REPORT .....</b>	<b>2</b>
<b>SECTION 2 MIDAMERICA ADMINISTRATIVE &amp; RETIREMENT SOLUTIONS, INC.’S ASSERTION.....</b>	<b>5</b>
<b>SECTION 3 COMPUTER DATA NETWORKS’ ASSERTION .....</b>	<b>8</b>
<b>SECTION 4 DESCRIPTION OF THE SYSTEM PROVIDED BY THE SERVICE ORGANIZATION .....</b>	<b>11</b>
OVERVIEW OF OPERATIONS .....	12
Company Background .....	12
Description of Services Provided.....	12
CONTROL ENVIRONMENT.....	16
Integrity and Ethical Values .....	16
Commitment to Competence .....	16
Management’s Philosophy and Operating Style.....	16
Organizational Structure and Assignment of Authority and Responsibility .....	17
Human Resources Policies and Practices.....	17
RISK ASSESSMENT .....	18
CONTROL OBJECTIVE AND RELATED CONTROL ACTIVITIES .....	18
MONITORING .....	19
INFORMATION AND COMMUNICATION SYSTEMS.....	19
Information Systems .....	19
Communication Systems .....	20
COMPLEMENTARY USER ENTITY CONTROLS .....	21
<b>SECTION 5 TESTING OF CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES PROVIDED BY THE SERVICE AUDITOR.....</b>	<b>22</b>
GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR.....	23
PHYSICAL SECURITY .....	24
ENVIRONMENTAL SECURITY.....	29
COMPUTER OPERATIONS.....	31
COMPUTER OPERATIONS - AVAILABILITY.....	32
INFORMATION SECURITY .....	34
DATA COMMUNICATIONS.....	45
DATA ENTRY .....	48
CONTRIBUTION PROCESSING .....	50
CUSTOMER SERVICE.....	52
DISTRIBUTION PROCESSING .....	54
VALUATION.....	62
PARTICIPANT STATEMENTS.....	65
HRA CLAIMS PROCESSING .....	67
TPA AND TPA SERVICES APPLICATION SERVICES.....	70
CLIENT IMPLEMENTATION .....	75
<b>SECTION 6 OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION.....</b>	<b>77</b>
DISASTER RECOVERY PLANNING .....	78

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

**INDEPENDENT SERVICE AUDITOR'S REPORT ON A DESCRIPTION OF MIDAMERICA  
ADMINISTRATIVE & RETIREMENT SOLUTIONS, INC.'S SYSTEM AND THE SUITABILITY OF THE  
DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS**

To MidAmerica Administrative & Retirement Solutions, Inc.:

We have examined MidAmerica Administrative & Retirement Solutions, Inc.'s ('MidAmerica' or 'the Company') and Computer Data Networks' ('CDN' or 'the Inclusive Subservice Organization') description of their Plan Administration Services System and Network Administration and Support Services System respectively at their Lakeland, Florida locations for processing user entities' transactions for the period October 1, 2014 through September 30, 2015, and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of MidAmerica's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design and operating effectiveness of such complementary user entity controls.

CDN is an independent service organization that provides Network Administration and Support Services System services to MidAmerica. MidAmerica's description includes a description of CDN's Network Administration and Support Services System used by MidAmerica to process transactions for its user entities, as well as relevant control objectives and controls of CDN.

In Section 2 and Section 3 of this report, MidAmerica and CDN have provided their assertions 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. MidAmerica and CDN are responsible for preparing the description and for the assertions, including the completeness, accuracy, and method of presentation of the description and the assertions, 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, 2014 through September 30, 2015.

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 the subservice organization and described in Section 2 and Section 3 respectively. 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 or subservice 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 or subservice organization may become inadequate or fail.

In our opinion, in all material respects, based on the criteria described in MidAmerica's and CDN's assertions in Section 2 and Section 3 of this report,

- the description fairly presents MidAmerica's Plan Administration Services System and CDN's computer processing services used by MidAmerica to process transactions for its user entities that were designed and implemented for the period October 1, 2014 through September 30, 2015.
- the controls related to the control objectives of MidAmerica and CDN 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, 2014 through September 30, 2015 and user entities applied the complementary user entity controls contemplated in the design of MidAmerica's controls for the period October 1, 2014 through September 30, 2015.
- the controls of MidAmerica and CDN that we tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively for the period October 1, 2014 through September 30, 2015.

The specific controls tested and the nature, timing, and results of those tests are listed in Section 5.

The information in Section 6 of management's description of MidAmerica's system, "Other Information Provided by the Service Organization," that describes disaster recovery planning, is presented by management of MidAmerica to provide additional information and is not a part of MidAmerica's description of its system made available to user entities during the period October 1, 2014 through September 30, 2015. Information about MidAmerica's disaster recovery planning has not been subjected to the procedures applied in the examination of the description of the system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the system and, accordingly, we express no opinion on it.

This report, including the description of tests of controls and results thereof in Section 5, is intended solely for the information and use of MidAmerica, user entities of MidAmerica's system during some or all of the period October 1, 2014 through September 30, 2015, 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.

The logo for A-LIGN, featuring a large, stylized letter 'A' followed by the word 'ALIGN' in a smaller, sans-serif font.

October 12, 2015  
Tampa, Florida

## **SECTION 2**

### **MIDAMERICA ADMINISTRATIVE & RETIREMENT SOLUTIONS, INC.'S ASSERTION**

## MidAmerica Administrative & Retirement Solutions, Inc.'s Assertion

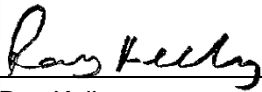
October 12, 2015

We have prepared the description of MidAmerica Administrative & Retirement Solutions, Inc.'s Plan Administration Services System for user entities of the system during some or all of the period October 1, 2014 through September 30, 2015, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief, that:

- a. The description fairly presents the Plan Administration Services System made available to user entities of the system during some or all of the period October 1, 2014 through September 30, 2015 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 Plan Administration Services 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 Plan Administration Services 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, 2014 through September 30, 2015 to achieve those control objectives. The criteria we used in making this assertion were that:
  - i. the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization;
  - ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and
  - iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.



---

Ray Kelly  
CEO  
MidAmerica Administrative &  
Retirement Solutions, Inc.

**SECTION 3**  
**COMPUTER DATA NETWORKS' ASSERTION**



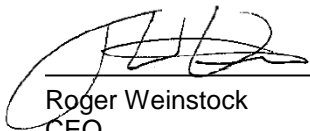
## Computer Data Networks' Assertion

October 12, 2015

We have prepared the description of aspects of Computer Data Networks' ('CDN' or 'the Inclusive Subservice Organization') Network Administration and Support Services System for MidAmerica Administrative & Retirement Solutions, Inc. ('MidAmerica' or 'the Company') and user entities of MidAmerica's Plan Administration Services system (description) during some or all of the period October 1, 2014 through September 30, 2015, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the systems themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief, that:

- a. The description fairly presents the aspects of CDN's computer processing system made available to MidAmerica and user entities of MidAmerica's Plan Administration Services System during some or all of the period October 1, 2014 through September 30, 2015, for processing their transactions. The criteria we used in making this assertion were that the description:
  - i. presents how the system made available to MidAmerica and user entities of MidAmerica's Plan Administration Services System was designed and implemented to process relevant transactions, including, if applicable:
    - (1) The types of services provided including, as appropriate, the classes of transactions processed.
    - (2) The procedures, within both automated and manual systems, by which services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information prepared for user entities.
    - (3) The related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
    - (4) How the system captures significant events and conditions, other than transactions.
    - (5) The process used to prepare reports and other information for user entities.
    - (6) The specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls contemplated in the design of 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 Plan Administration Services System, while acknowledging that the description is presented to meet the common needs of a broad range of user entities of the systems and their financial statement auditors, and may not, therefore, include every aspect of the Plan Administration Services System that each individual user entity of the system and its auditor may consider important in its own particular environment.

- iii. includes relevant details of the changes to the Plan Administration Services System during the period covered by the description.
- b. The controls related to the control objectives stated in the description that relate to aspects of CDN's system made available to MidAmerica were suitably designed and operating effectively for the period October 1, 2014 through September 30, 2015, to achieve those control objectives. The criteria we used in making this assertion were that:
  - i. The risks that threaten the achievement of the control objectives stated in the description have been identified by management;
  - ii. The controls identified in the description would, if operating as described provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and
  - iii. The controls were consistently applied as designed, and manual controls were applied by individuals who have the appropriate competence and authority.



\_\_\_\_\_  
Roger Weinstock  
CEO  
Computer Data Networks

**SECTION 4**  
**DESCRIPTION OF THE SYSTEM PROVIDED**  
**BY THE SERVICE ORGANIZATION**

## OVERVIEW OF OPERATIONS

### Company Background

MidAmerica Administrative and Retirement Solutions, Inc. and Subsidiaries (MidAmerica) provides employee benefit programs to approximately 2,400 plan sponsors and over a half million employees across the country. Originally formed in 1995, MidAmerica focused primarily on providing Internal Revenue Code Section 3121 Social Security opt-out programs to governmental employers. The core business has grown and has expanded to include Health Reimbursement Arrangements, Flexible Spending Account administration, Special Pay programs, Governmental Accounting Standards Board (GASB) 45 programs, and more recently, independent 403(b) and 457 third party administration and common remitting services.

### Description of Services Provided

#### *Health Reimbursement Arrangement (HRA)*

HRAs allow the employer to make deposits on behalf of the active employees and /or retirees. Deposits are made tax-free, carry over from year to year, earn interest tax free and are used for qualified medical expenses and premiums. The plan can also be used in conjunction with the special pay plan.

Plan documentation, implementation materials and plan administration are provided to the employer. HRA plans are structured according to the Internal Revenue Service (IRS) Revenue Ruling 2002-41 and IRS Notice 2002-45.

#### *Flexible Spending Account (FSA)*

FSAs, oftentimes called Section 125 Cafeteria plans, were formally created by Internal Revenue Code 125 of the Revenue Act of 1978. The Act allowed employees to set aside money on a pre-tax basis to pay for certain expenses. Expenses eligible for reimbursement include required employee contributions to an employer sponsored health care plan, dependent care expenses and any health care expenses not covered by the employer health care plan. Examples of these expenses include co-payments, deductibles, prescription drug purchases, eyeglasses and dental expenses or any other eligible uncovered medical expenses. Money deposited in FSA's must be used in the year it is deposited or the remaining balance is forfeited. An exception to this time period includes any applicable claims run out period as outlined in the plan's document. As well, in 2014, the IRS amended the "use or lose" rule stating, FSAs that don't include a run out period will have the option of allowing employees to roll over up to \$500 of unused funds at the end of this plan year.

#### *Special Pay Plan*

The special pay plan is designed to handle forms of compensation in a tax-advantaged manner. These forms of compensation typically include unused sick leave and unused vacation pay. Payments may also be based on years of service, severance and other retirement incentives.

#### *Accumulation Program for Part-time and Limited-service Employees (APPLE) and Social Security 3121 Alternative Plan*

In 1990, the Omnibus Budget Reconciliation Act was passed. Government entities who exercised their Social Security Section 218 exclusion allowance were provided the option of giving their part-time, temporary and seasonal employees a meaningful, defined benefit contribution, retirement alternative to Social Security. The Plan is structured as an Internal Revenue Code Section 401(a) or 457 plan.

### *Employer Sponsored 403(b) Plan*

The Employer Sponsored 403(b) Plan is designed to provide a tax advantaged savings vehicle to pay for retiree health care expenses. Other payments may be contributed to the plan based on years of service, severance and other retirement incentives. The employee's contributions are made on a pre-tax basis. The employee also saves the 7.65% Social Security and Medicare tax. Individual IRS limits on Section 403(b) or Section 457 contributions are typically not affected.

A retiring employee (or surviving spouse) can either take a partial or lump sum distribution, or roll their funds into an individual retirement account (IRA) or another employer's qualified plan. There is no 10% penalty if the employee is over the age of 55 when he/she retires.

### *403(b) Third Party Administrator (TPA) and Common Remitting Services*

In 2009 the IRS issued new 403(b) regulations that require significant additional oversight by employers, including plan documentation, limits testing, and oversight of hardships, loans and eligibility. MidAmerica developed a service offering to all employers to largely outsource the new compliance requirements:

- Vendor oversight which includes help with selection and paring down of the best vendors. MidAmerica will review and approve all plan activity, including salary reduction agreements (SRAs), loans, hardships, distributions and contract exchanges/transfers to ensure compliance with the new regulations and that the vendor conforms to the plan provisions and investment requirements
- Plan administration and compliance which provides a plan document, monitoring of loans, hardships, eligibility, limits under sections 402(g) and 415, guidance regarding Universal Availability, and Form 5500 and SAR preparation. MidAmerica will process contributions and distributions in addition to monitoring vendor performance to keep the plan and documents current and in compliance
- Common remitting, which includes working with payroll departments to streamline employees' investment elections and payroll contributions to multiple plan vendors, thereby reducing the employer's administrative burden
- Employee and employer communications which includes a custom web portal for all eligible participants and provides the plan's sponsor with an annual report on vendor compliance, testing and plan level highlights

### *Employee Benefit Trust*

Many employers provide other post-employment benefits (OPEB) such as continuing health care coverage for their employees. When an employee retires, those benefits are usually paid out of the employer's current operational budget. GASB, through Statement 45, requires the disclosure of this liability on the financial statement and recommends that the employer begin funding this liability. Steps must be taken to minimize the impact of this liability, including funding. Funding sets aside assets to offset the liability on the financial statement. GASB recommends establishing an irrevocable Employee Benefit Trust for this purpose. MidAmerica provides everything that is needed to establish a Trust including an employer resolution, implementation documents and Trust administration.

### *Significant Events*

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

## *Functional Areas of Operation*

In order to efficiently perform its plan administration services and maintain a separation of duties, MidAmerica is organized into the following operational areas:

- Executive management - responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives
- IT department - manages, monitors, and supports internal information systems with the support of the third party vendor, Computer Data Services (CDN)
- Accounting department - responsible for processing distribution checks and performing reconciliations related to services provided to user entities and provides financial and regulatory reporting and compliance
- 403(b) TPA team - responsible for vendor oversight, plan administration, and compliance monitoring
- Contribution processing team - responsible for the processing of contributions as received from employers and plan participants
- Distribution processing team - responsible for the processing of distributions, including making adjudication decisions for certain plan types
- Plan administration team - responsible for overall plan administration, trading, and reconciliation of assets with financial partners; also responsible for issuing periodic plan statements
- Customer service - provide customer service including the maintenance of toll-free telephone lines for calls from program participants

## *Procedures*

### Physical Security

A physical security policy is in place to guide personnel in access practices. The MidAmerica office suite is located within a multi-tenant office building. The office suite doors are locked at all times. The front entrance is monitored by a receptionist during normal business hours and visitors are required to sign in prior to gaining access. A badge access system is also in place to control access to the office suite 24 hours per day. Employees are assigned access levels within the badge access system and only certain employees have 24 hour access to the office suite. Administrative access to the badge system is only provided to the senior vice president of operations and the IT supervisor. Badge access permissions are reviewed on a quarterly basis by the senior vice president of operations. The server room door is secured via a cipher code lock and restricted to management and CDN IT personnel.

### Environmental Security

The server room includes fire detection and suppression equipment that include a fire alarm system, water sprinklers, and a handheld fire extinguisher which is inspected by a third party specialist on an annual basis. The server room contains a dedicated air conditioning unit to maintain air temperature and humidity levels. An environmental monitoring application is configured to perform self-tests of the UPS system on a semi-monthly basis. The application is configured to send e-mail alerts to IT personnel when predefined temperature thresholds are exceeded. Production equipment is also connected to an uninterruptible power supply (UPS) system to provide temporary power in the event of a power failure. Production IT equipment in the server room is placed in racks which elevate the equipment off of the floor to protect from localized flooding.

### Computer Operations

Policies are in place to guide personnel in backup and restoration processes. Automated backup systems are configured and monitored to ensure that data and systems are backed up and replicated timely. System administrators are notified of each backup status whether successful or failed events occur. Backup data files are replicated to a third party data center.



Documented incident response policies and procedures are in place to guide personnel in reporting and responding to major information technology incidents. Monitoring is in place to help detect network and system level failures. Antivirus software is installed on Windows servers and desktops to monitor for malware. In the event of an outage, trouble tickets are automatically created and notifications are configured and sent to a distribution group including both CDN and MidAmerica personnel in real time via e-mail. Once alerted, the CDN engineers take corrective action to restore services.

### Information Security

Active Directory controls access to the network domain and requires users to enter a unique account and valid password. Password parameters such as password expiration, minimum length, password history, password complexity and account lockout controls are enforced on user accounts. User accounts are assigned to predefined access roles to restrict access to certain functions. Windows web server and database server authentication is derived from the network domain. Administrative access to the network domain, the server operating systems, the Oracle and SQL databases, and the Relius application are restricted to authorized personnel that include management and CDN IT personnel. Terminated employee access to the network domain and systems is revoked as a component of the termination process.

The Relius administration system, commercially licensed software, utilizes both a Microsoft SQL Server database and an Oracle database. The TPA Services Application and 403(b) TPA services application is a custom-developed browser-based application that utilizes a Microsoft SQL Server database. Administrative access to the databases is restricted to authorized personnel that include management and CDN IT personnel.

The Relius administration application and the TPA Services Application both require a valid user account name and password. The Relius administration application enforces certain password parameters that include minimum length, password expiration, password complexity and account lockout controls. Administrative access within the TPA services application is restricted to authorized personnel that include management and senior business representatives.

### Data Communications

A Sophos UTM firewall is in place to restrict traffic to network. Specific firewall rules are configured to allow certain services, ports and protocols and deny traffic not specifically allowed. Network address translation is configured to translate internally routable IP addresses via “friendly” host object names. CDN manages and administers the firewall system. An encrypted virtual private network (VPN) is in place to provide remote access to production. Only certain employees have the ability to remotely connect over the VPN and administrative access to the VPN console is restricted. Finally, an intrusion protection system (IPS) is in place to monitor the production network for signatures recognized by the IPS.

### Data Entry

As contribution monies are received, the mail receiving clerk date stamps and enters the information on a tracking spreadsheet. The monies are then sent to the accounting department that also maintains a check log. The accounting assistant reconciles the mail receipt log and the check log on a monthly basis.

### **Boundaries of the System**

The scope of this report includes MidAmerica’s Plan Administration services performed in the Lakeland, Florida facility.

### **Subservice Organizations**

This report also includes the Managed Services provided by CDN at the Lakeland, Florida facilities.

## **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**

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of MidAmerica's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of MidAmerica's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

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

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

### **Commitment to Competence**

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

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

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements
- Skills testing is utilized during the hiring process to qualify the skills of personnel for certain positions
- Training is provided to maintain the skill level of personnel in certain positions

### **Management's Philosophy and Operating Style**

MidAmerica's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

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

- Management is periodically briefed on regulatory and industry changes affecting the services provided
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole
- A designated Health Insurance Portability and Accountability Act (HIPAA) coordinator monitors compliance with HIPAA regulations and MidAmerica's documented HIPAA Policy

### **Organizational Structure and Assignment of Authority and Responsibility**

MidAmerica's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

MidAmerica's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are communicated to employees and updated as needed.

### **Human Resources Policies and Practices**

MidAmerica'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 who ensures the service organization is operating at maximum efficiency. MidAmerica's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

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

- Pre-hire screening procedures are in place and are documented in a new hire checklist
- A new hire orientation checklist must be signed by each new employee after they attend orientation on their first day of employment
- Evaluations for each employee are performed after 90 days of employment and on a semi-annual basis
- Customer service representatives receive semi-annual quality assurance reviews
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist
- Employees that have access to protected health information (PHI) are required to read the HIPAA policies and procedures and sign an acknowledgement form indicating that they have read and understand the policies and procedures
- A formal HIPAA training program is in place to educate employees on HIPAA regulations
- Employees are educated regarding sensitive document controls. A secure shredding system is in place to manage the disposal of discarded sensitive documents
- Vendors and subcontractors who have access to PHI are required to sign business associate agreements that address HIPAA regulations

## **RISK ASSESSMENT**

MidAmerica's risk assessment process identifies and manages risks that could potentially affect MidAmerica's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. MidAmerica identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by MidAmerica and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

MidAmerica has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. MidAmerica attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

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

### **Integration with Risk Assessment**

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

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

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

## MONITORING

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. MidAmerica's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

### On-Going Monitoring

Senior management is extremely involved in the day to day operations of the company and provides for hands on monitoring. Management meets weekly to discuss outstanding items and issues that provides for real time monitoring of operational activities. Regular conference calls with vendors and client organizations assist in the monitoring process.

Management assesses the quality of internal control performance on an ongoing basis by implementing and performing various review activities that include the following:

- Quarterly review of badge access assignments for accuracy
- Periodic environmental equipment inspections
- Monitoring of IT infrastructure issues and incidents
- Random customer service call monitoring and evaluations
- Periodic customer service satisfaction surveys
- Reconciliations are performed on a daily and monthly basis throughout the plan administration process

### Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

## INFORMATION AND COMMUNICATION SYSTEMS

### Information Systems

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

#### *Infrastructure*

Primary infrastructure used to provide MidAmerica's Plan Administration system includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
Virtual Hosts	HP Proliant DL380	HP Proliant DL380
SAN	NetApp CS2240	iSCSI & CIFS Storage for the Virtual Hosts and Shares
Backup	Barracuda Backup 890	Daily Full VMDK Backup of the Entire System with local and offsite data storage

Primary Infrastructure		
Hardware	Type	Purpose
Virtual Hosts	HP Proliant DL380	Virtualization layer of the Network running on VMWare vSphere 5.5
SAN	NetApp CS2240	iSCSI & CIFS Storage for the Virtual Hosts and Shares
Backup	Barracuda Backup 890	Daily Full VMDK Backup of the Entire System with local and offsite data storage
E-mail Archiver	Barracuda Message Archiver 350	E-mail Archiving and retention of all Internal and External E-mails sent or received
NAS	FreeNAS Server	Barracuda Message Archiver Backups and Relius Database Export storage
Scanning Server	Custom Built Server	Ademero Content Central Server for scanning and indexing files
Wireless	TrendNet Wireless AP	Internet Only Wireless connected to the Sophos Firewall. Traffic is only allowed to the Internet. No Internal Network Access is available

#### Software

Primary software used to provide MidAmerica's Plan Administration system includes the following:

Primary Software	
Software	Purpose
OpenFire Server	Instant Messaging Server for internal use only, available from inside the network only or while connected to the SSL VPN
Allegeus	Administration system for HSA and HRA plans
Content Central	Document management software used to translate paper documents into electronic storage
MARS Utilities	Developed internally, the software is used to pull information from Relias to create direct deposit and check files
Relias	Administration system that houses the majority of the client data, with the exception of the plans hosted in Allegeus and Relevant Remitter
Relevant Remitter	Administration system for TPA clients

#### Communication Systems

Communication is an integral component of MidAmerica's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At MidAmerica, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization.

Additionally, town hall meetings are held bi-annually in each geographic location to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the town hall meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate MidAmerica personnel via e-mail messages.

## **COMPLEMENTARY USER ENTITY CONTROLS**

MidAmerica'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 Trust Services Principles related to MidAmerica's services to be solely achieved by MidAmerica's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of MidAmerica's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Principles 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.

1. User entities are responsible for ensuring that user IDs and passwords are assigned to only authorized individuals.
2. User entities are responsible for ensuring the confidentiality of any user IDs and passwords used to access MidAmerica's systems.
3. User entities are responsible for ensuring that data submitted to MidAmerica is complete, accurate and timely.
4. User entities are responsible for ensuring that their data are formatted in accordance with agreed upon standards.
5. User entities are responsible for submitting contribution payments in an accurate and timely manner.
6. User entities are responsible for reviewing and approving the distribution authorization lists sent by MidAmerica.
7. User entities are responsible for reviewing distribution request forms for completeness before they are sent to MidAmerica.
8. User entities are responsible for submitting the data needed to perform 402(g) and 415 compliance testing.
9. User entities are responsible for immediately notifying MidAmerica of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

## **SECTION 5**

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



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

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

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

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

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

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

**CONTROL AREA 1**

**PHYSICAL SECURITY**

Control Objective Specified by the Service Organization:

Control activities 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	A badge access system is in place to restrict access to the office suite.	Observed the exterior office entrances to determine that a badge access system was in place to restrict access to the office suite.	No exceptions noted.
1.2	A digital camera surveillance system is in place to monitor and record activity at the entrance of the secondary office off Main Street.	Observed the camera at the main entrance to the facility to determine that a digital camera surveillance system was in place to monitor and record activity at the entrance of the secondary office off Main Street.	No exceptions noted.
1.3	A physical security policy is in place to guide personnel in determining access rights.	Inspected the physical security policy to determine that a physical security policy was documented.	No exceptions noted.
1.4	A receptionist monitors and controls access to the office suite during normal business hours.	Observed the suite entrance to determine that a receptionist monitored and controlled access to the office suite during normal business hours.	No exceptions noted.
1.5	Access to the Main Street office is restricted by the use of a keypad with a 4 digit pin required for entry.	Observed an employee enter a 4 digit code in the elevator to determine that access to the Main Street office was restricted by the use of a keypad with a 4 digit pin required for entry.	No exceptions noted.
1.6	Administrative access within the badge access system is restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• Senior vice president of operations</li> <li>• IT supervisor</li> </ul>	Inspected the badge access system administrator listing to determine that administrative access within the badge access system was restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• Senior vice president of operations</li> <li>• IT supervisor</li> </ul>	No exceptions noted.



**CONTROL AREA 1                      PHYSICAL SECURITY**

Control Objective Specified by the Service Organization:      Control activities 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
1.9	Exterior doors to the office suite are locked at all times.	<p>Inspected the termination checklist and badge access listing for a sample of employees terminated during the review period to determine that badge access was revoked for each employee sampled.</p> <p>Inquired of the Information Technology Department Supervisor regarding office suite security to determine that exterior doors to the office suite were locked at all times.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
1.10	Management maintains video back-ups of surveillance footage for a minimum of 60 days.	<p>Observed the office suite entrances to determine that exterior doors to the office suite were locked during business hours.</p> <p>Inspected the configurations settings of the surveillance system and a example image to determine that management maintained video back-ups of surveillance footage for a minimum of 60 days.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
1.11	Sensitive documents are discarded in a locked shredding bins strategically located throughout the facility.	Inspected the contract with a third party shredding company and invoices for a sample of months to determine that sensitive documents were discarded in a locked shredding bins strategically located throughout the facility.	No exceptions noted.

**CONTROL AREA 1**

**PHYSICAL SECURITY**

Control Objective Specified by the Service Organization:

Control activities 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
1.12	The senior vice president of operations reviews badge access permissions on a quarterly basis to help ensure that badge access permissions are authorized for each employee.	<p>Inquired of the senior vice president of operations regarding the badge access review process to determine that the senior vice president of operations reviewed badge access permissions on a quarterly basis to help ensure that badge access permissions were authorized for each employee.</p> <p>Inspected the badge access review documentation for a sample of quarters during the review period to determine that the senior vice president of operations performed a badge access review for each quarter sampled.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
1.13	<p>The server room door is secured via a cipher code lock. Knowledge of the server room door cipher code is restricted to persons holding the following positions:</p> <ul style="list-style-type: none"> <li>• Senior VP of operations</li> <li>• VP of compliance and business development</li> <li>• VP of finance and administration</li> <li>• TPA services director</li> <li>• IT department supervisor</li> <li>• Systems analyst</li> <li>• CDN IT personnel (3)</li> </ul>	<p>Inspected a listing of personnel with knowledge of the server room cipher lock code with the assistance of the IT supervisor to determine that knowledge of the server room door cipher lock code was restricted to persons holding the following positions:</p> <ul style="list-style-type: none"> <li>• Senior VP of operations</li> <li>• VP of compliance and business development</li> <li>• VP of finance and administration</li> <li>• IT department supervisor</li> <li>• Systems analyst</li> <li>• CDN IT personnel (3)</li> </ul>	No exceptions noted.

**CONTROL AREA 1                      PHYSICAL SECURITY**

Control Objective Specified by the Service Organization:      Control activities 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
1.14	Visitors are required to sign a visitors' log upon entering the office suite.	<p>Observed the server room entrance to determine that the server room door was secured via a cipher code lock.</p> <p>Inspected visitor logs for a sample of months during the review period to determine that a sign-in log was utilized to document visitor's access to the suite for each month sampled.</p> <p>Observed the visitor access process to determine that visitors were required to sign a visitors log upon entering the office suite.</p> <p>Inspected visitor logs for a sample of months during the review period to determine that a sign-in log was utilized to document visitor's access to the suite for each month sampled.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**CONTROL AREA 2 ENVIRONMENTAL SECURITY**

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

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.1	A dedicated air conditioning unit is in place to maintain air temperature and humidity levels within the server room.	<p>Inquired of the IT supervisor regarding server room air conditioning to determine that a dedicated air conditioning unit was in place to maintain air temperature and humidity levels within the server room.</p> <p>Observed the server room to determine that a dedicated air conditioning unit was in place.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
2.2	A third party specialist is contracted to inspect and service the fire alarm system and water sprinkler system on an annual basis. An inspection report is retained as evidence of the completed inspection.	Inspected third party specialist inspection report for the fire alarm system and water sprinkler system on an annual basis to determine that an inspection report was completed during the review period and retained as evidence of the completed inspection.	No exceptions noted.
2.3	A third party specialist is contracted to inspect and service the handheld fire extinguishers on an annual basis.	Inspected third party specialist inspection report for the handheld fire extinguishers to determine that an inspection report was completed during the review period and was retained as evidence of the completed inspection.	No exceptions noted.
2.4	An environmental monitoring application is configured to perform self-tests of the UPS system on a semi-monthly basis.	Inspected the environmental monitoring application configurations to determine that an environmental monitoring application was configured to perform self-tests of the UPS system on a semi-monthly basis.	No exceptions noted.

**CONTROL AREA 2**

**ENVIRONMENTAL SECURITY**

Control Objective Specified by the Service Organization:

Control activities provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threat.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.5	An environmental monitoring application is configured to send e-mail alerts to IT personnel when predefined temperature thresholds are exceeded.	Inspected the environmental monitoring application configurations to determine that an environmental monitoring application was configured to send e-mail alerts to IT personnel when predefined temperature thresholds were exceeded.	No exceptions noted.
2.6	Production IT equipment in the server room is placed in racks which elevate the equipment off of the floor to protect from localized flooding.	Observed the server room to determine that production IT equipment in the sever room was placed in racks which elevated the equipment off of the floor to protect from localized flooding.	No exceptions noted.
2.7	Production IT equipment is connected to uninterruptible power supply (UPS) systems to provide backup power in the event of a primary power failure, and to mitigate the risk of power surges impacting production infrastructure.	Inquired of the IT supervisor regarding UPS systems to determine that production IT equipment was connected to UPS systems to provide backup power in the event of a primary power failure, and to mitigate the risk of power surges impacting production infrastructure.	No exceptions noted.
2.8	The server room is equipped with the following fire detection and suppression equipment: <ul style="list-style-type: none"> <li>• Fire alarm system</li> <li>• Water sprinklers</li> <li>• Handheld fire extinguisher</li> </ul>	Observed the production IT equipment to determine that the equipment was connected to UPS systems.  Observed the server room to determine that the server room was equipped with the following fire detection and suppression equipment: <ul style="list-style-type: none"> <li>• Fire alarm system</li> <li>• Water sprinklers</li> <li>• Handheld fire extinguisher</li> </ul>	No exceptions noted.



**CONTROL AREA 3**

**COMPUTER OPERATIONS**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance of timely system backups of critical files, off-site backup storage, and regular off-site rotation of backup files.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.1	Documented data backup and restoration policies and procedures are in place to guide personnel in the backup and restoration processes.	Inspected the data backup and restoration policies and procedures to determine that backup and restoration policies and procedures were documented.	No exceptions noted.
3.2	IT personnel utilize an automated backup system to perform full backups of production data on a daily basis, Monday through Friday.	Inspected the automated backup system configurations and example backup logs generated during the review period to determine that an automated backup system was configured to perform full backups of production data on a daily basis, Monday through Friday.	No exceptions noted.
3.3	The automated backup system is configured to replicate backup data to a third party data center.	Inspected the automated backup system data replication configurations to determine that the automated backup system was configured to replicate backup data to a third party data center.	No exceptions noted.
3.4	The automated backup system is configured to send backup completion status e-mail notifications to the following positions: <ul style="list-style-type: none"> <li>• IT supervisor</li> <li>• Systems analyst</li> <li>• CDN IT personnel</li> </ul>	Inspected the automated backup system notification configurations and an example backup completion status e-mail generated during the review period to determine that the automated backup system was configured to send backup completion status e-mail notifications to the following positions: <ul style="list-style-type: none"> <li>• IT supervisor</li> <li>• Systems analyst</li> <li>• CDN IT personnel</li> </ul>	No exceptions noted.

**CONTROL AREA 4**

**COMPUTER OPERATIONS - AVAILABILITY**

Control Objective Specified by the Service Organization: Control activities 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	An enterprise monitoring application is configured to send e-mail notifications of production outages to CDN IT personnel.	Inspected the enterprise monitoring application configurations and an example e-mail notification generated during the review period to determine that an enterprise monitoring application sent e-mail notifications of production outages to CDN IT personnel.	No exceptions noted.
4.2	Antivirus software is installed on Windows servers and workstations to protect against certain virus definitions recognized by the software.	Inspected the antivirus software configurations to determine that antivirus software was installed on Windows servers and workstations to protect against certain virus definitions recognized by the software.	No exceptions noted.
4.3	Documented incident response policies and procedures are in place to guide personnel in reporting and responding to major information technology incidents.	Inspected the incident response procedures to determine that incident response policies and procedures were documented and included procedures for reporting and responding to incidents.	No exceptions noted.
4.4	IT personnel log operational issues into a ticketing system and assign personnel to monitor the status of the issues.	Inquired of the IT supervisor regarding the ticketing system to determine that IT personnel logged operational issues into a ticketing system and assigned personnel to monitor the status of the issues.	No exceptions noted.
		Inspected a listing of operational issues logged in the ticketing system during the review period to determine that operational issues were logged into a ticketing system.	No exceptions noted.

**CONTROL AREA 4****COMPUTER OPERATIONS - AVAILABILITY**

Control Objective Specified  
by the Service Organization:

Control activities provide reasonable assurance that systems are maintained in a manner that helps ensure system availability.

<b>Control Point</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
4.5	The antivirus software is configured to update virus definitions every hour.	Inspected the antivirus software configurations to determine that the antivirus software was configured to update virus definitions every hour.	No exceptions noted.

**CONTROL AREA 5**

**INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities 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
<b>Network Authentication and Access</b>			
5.1	Users are required to authenticate via a user account and password before being granted access to the network domain.	Inspected a listing of network user accounts and the network authentication configurations to determine that users were required to authenticate via a network user account and password before being granted access to the network domain.	No exceptions noted.
5.2	The network domain is configured to enforce the following password requirements: <ul style="list-style-type: none"> <li>• Minimum length</li> <li>• Expiration interval</li> <li>• Password history</li> <li>• Password complexity</li> <li>• Invalid login attempt lockout threshold</li> </ul>	Inspected the network password and account lockout configurations to determine that the network domain was configured to enforce the following password requirements: <ul style="list-style-type: none"> <li>• Minimum length</li> <li>• Expiration interval</li> <li>• Password history</li> <li>• Password complexity</li> <li>• Invalid login attempt lockout threshold</li> </ul>	No exceptions noted.
5.3	Administrative access within the network domain is restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• IT department supervisor</li> <li>• Systems analyst</li> <li>• CDN IT personnel</li> </ul>	Inspected the network administrator listing to determine that administrative access within the network domain was restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• IT department supervisor</li> <li>• Systems analyst</li> <li>• CDN IT personnel</li> </ul>	No exceptions noted.

**CONTROL AREA 5****INFORMATION SECURITY**

Control Objective Specified by the Service Organization:

Control activities 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
5.4	Access to the network domain is revoked as a component of the termination process.	Inspected the termination checklist and the domain user account listing for a example of employees terminated during the review period to determine that access to the network domain was revoked for each employee sampled.	No exceptions noted.
<b>Web and Database Server Operating System Access</b>			
5.5	Administrative access within the web and database server operating systems is restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• IT supervisor</li> <li>• Systems analyst</li> <li>• CDN IT personnel</li> <li>• Third party contractor</li> </ul>	Inspected the server operating system administrator listing for a sample of production servers and noted that administrative access within the sample web and database servers' operating systems was restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• IT supervisor</li> <li>• Systems analyst</li> <li>• CDN IT personnel</li> <li>• Third party contractor</li> </ul>	No exceptions noted.
<b>SQL Database Authentication and Access</b>			
5.6	Administrative access within the database is restricted to a shared user account accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• IT supervisor</li> <li>• Systems analyst</li> <li>• Third party contractor</li> </ul>	Inquired of the IT supervisor regarding database access to determine that administrative access within the database was restricted to a shared user account accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• IT supervisor</li> <li>• Systems analyst</li> <li>• Third party contractor</li> </ul>	No exceptions noted.

**CONTROL AREA 5**

**INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities 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
		Inspected the listing of user accounts with administrative access to the database to determine that administrative access within the database was restricted to a shared user account accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• IT supervisor</li> <li>• Systems analyst</li> <li>• Third party contractor</li> </ul>	No exceptions noted.
<b>Oracle Database Authentication and Access</b>			
5.7	Users are required to authenticate via a user account and password before being granted access to the database.	Inspected the database authentication configuration to determine that users were required to authenticate via a user account and password before being granted access to the database.	No exceptions noted.
5.8	Administrative access within the database is restricted to default user accounts accessible by persons holding the following position: <ul style="list-style-type: none"> <li>• IT department supervisor</li> <li>• Systems analyst</li> </ul>	Inquired of the IT supervisor regarding database access to determine that administrative access within the database was restricted to default user accounts accessible by persons holding the following position: <ul style="list-style-type: none"> <li>• IT department supervisor</li> <li>• Systems analyst</li> </ul>	No exceptions noted.

**CONTROL AREA 5**

**INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities 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
		Inspected the listing of database roles and privileges to determine that administrative access within the database was restricted to default user accounts accessible by persons holding the following position: <ul style="list-style-type: none"> <li>• IT department supervisor</li> <li>• Systems analyst</li> </ul>	No exceptions noted.
<b>Application Level Access</b>			
5.9	Access to the administration system application is revoked as a component of the termination process.	Inquired of the IT supervisor regarding access revocation to determine that access to the administration system application was revoked as a component of the termination process.  Inspected the termination checklist and administration system application user account listing for a sample of employees terminated during the review period to determine that access to the administration system application was revoked for each employee sampled.	No exceptions noted.  No exceptions noted.
5.10	Access to the TPA services application is revoked as a component of the termination process.	Inquired of the IT supervisor regarding access revocation to determine that access to the TPA services application was revoked as a component of the termination process.	No exceptions noted.

**CONTROL AREA 5                    INFORMATION SECURITY**

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

<b>Control Point</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		Inspected the termination checklist and TPA services application user account listing for a sample of employees terminated during the review period to determine that access to the TPA services application was revoked for each employee sampled.	No exceptions noted.



**CONTROL AREA 5**

**INFORMATION SECURITY**

Control Objective Specified by the Service Organization:

Control activities 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
5.11	Administrative access within the Alegeus application is restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• Vice President of Compliance &amp; Business Development</li> <li>• Correspondence/Quality Assurance Department Supervisor</li> <li>• Account Services</li> <li>• Accounting Account Assistant</li> <li>• Health and Welfare Department Supervisor</li> <li>• Health and Welfare Administrative Assistant</li> <li>• Compliance Director</li> <li>• Alegeus Admin</li> <li>• Plan Implementation Department Supervisor</li> <li>• Plan Implication Specialist</li> <li>• IT Department Supervisor</li> <li>• IT System Analyst</li> <li>• Plan Implementation Specialist Department Supervisor</li> <li>• Accounting Department Supervisor</li> </ul>	Inspected the listing of Alegeus application administrator accounts to determine that administrative access within the Alegeus application was restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• Vice President of Compliance &amp; Business Development</li> <li>• Correspondence/Quality Assurance Department Supervisor</li> <li>• Account Services</li> <li>• Accounting Account Assistant</li> <li>• Health and Welfare Department Supervisor</li> <li>• Health and Welfare Administrative Assistant</li> <li>• Compliance Director</li> <li>• Alegeus Admin</li> <li>• Plan Implementation Department Supervisor</li> <li>• Plan Implementation Specialist</li> <li>• IT Department Supervisor</li> <li>• IT System Analyst</li> <li>• Plan Implementation Specialist Department Supervisor</li> <li>• Accounting Department Supervisor</li> </ul>	No exceptions noted.

**CONTROL AREA 5**

**INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities 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
5.12	Administrative access within the Content Central application is restricted to user accounts accessible by persons holding the following positions.	Inspected the listing of Content Central application administrator accounts to determine that administrative access within the Content Central application was restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• IT Department Supervisor</li> <li>• IT System Analyst</li> <li>• Plan Administration Department Supervisor</li> <li>• Health and Welfare Department Supervisor</li> </ul>	No exceptions noted.
5.13	Administrative access within the ShoreTel application is restricted to user accounts accessible by persons holding the following positions.	Inspected the listing of ShoreTel application administrator accounts to determine that administrative access within the ShoreTel application was restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• Senior HRA/FSA Distribution Processor</li> <li>• IT Department Supervisor</li> <li>• IT Systems Analyst</li> <li>• Account Services Department Supervisor</li> <li>• Account Services Senior Bilingual Account Services representative</li> </ul>	No exceptions noted.

**CONTROL AREA 5**

**INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities 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
5.14	Administrative access within the TPA services application is restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• Vice President of Compliance &amp; Business Development</li> <li>• Vice President of Administration &amp; Finance</li> <li>• Senior Account Services Representative</li> <li>• Accounting Department Supervisor</li> <li>• Correspondence/Quality Assurance</li> <li>• Health and Welfare Department Supervisor</li> <li>• IT Department Supervisor</li> <li>• IT Systems Analyst</li> <li>• 403(b) TPA Services Department Supervisor</li> <li>• 403(b) TPA Senior Account Manager</li> <li>• Plan Implementation Specialist</li> <li>• Plan Implementation Administrative Assistant</li> <li>• Compliance Director</li> </ul>	Inspected the listing of TPA services application administrator accounts to determine that administrative access within the TPA services application was restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• Vice President of Compliance &amp; Business Development</li> <li>• Vice President of Administration &amp; Finance</li> <li>• Senior Account Services Representative</li> <li>• Accounting Department Supervisor</li> <li>• Correspondence/Quality Assurance</li> <li>• Health and Welfare Department Supervisor</li> <li>• IT Department Supervisor</li> <li>• IT Systems Analyst</li> <li>• 403(b) TPA Services Department Supervisor</li> <li>• 403(b) TPA Senior Account Manager</li> <li>• Plan Implementation Specialist</li> <li>• Plan Implementation Administrative Assistant</li> <li>• Compliance Director</li> </ul>	No exceptions noted.

**CONTROL AREA 5****INFORMATION SECURITY**

Control Objective Specified by the Service Organization:

Control activities 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
5.15	Administrative access within the administration application is restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• VP of compliance and business development</li> <li>• VP of administration and finance</li> <li>• IT department supervisor</li> <li>• HRA/FSA administrative department supervisor</li> </ul>	Inspected the listing of administration application user accounts to determine that administrative access within the administration application was restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• VP of compliance and business development</li> <li>• VP of administration and finance</li> <li>• IT department supervisor</li> <li>• HRA/FSA administrative department supervisor</li> </ul>	No exceptions noted.
5.16	Application users are required to authenticate via a password before being granted access to the ShoreTel application.	Inspected the application authentication configurations to determine that application users were required to authenticate via a password before being granted access to the ShoreTel application.	No exceptions noted.
5.17	Application users are required to authenticate via a user account and password before being granted access to the TPA services application.	Inspected the application authentication configurations to determine that users were required to authenticate via a user account and password before being granted access to the TPA services application.	No exceptions noted.
5.18	Application users are required to authenticate via a user account and password before being granted access to the administration system application.	Inspected the application authentication configurations to determine that users were required to authenticate via a user account and password before being granted access to the administration application.	No exceptions noted.

**CONTROL AREA 5****INFORMATION SECURITY**

Control Objective Specified by the Service Organization:

Control activities 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
5.19	Application users are required to authenticate via a username and password before being granted access to the Alegeus application.	Inspected the application authentication configurations to determine that application users were required to authenticate via a username and password before being granted access to the Alegeus application.	No exceptions noted.
5.20	Application users are required to authenticate via username and password before being granted access to the Content Central application.	Inspected the Content Central login screen to determine that application users were required to authenticate via username and password before being granted access to the Content Central application.	No exceptions noted.
5.21	<p>The administration system application is configured to enforce the following password requirements:</p> <ul style="list-style-type: none"> <li>• Minimum length</li> <li>• Expiration interval</li> <li>• Complexity requirements</li> <li>• Invalid login attempt lockout threshold</li> </ul>	<p>Inspected the application password configurations to determine that the administration system application was configured to enforce the following password requirements:</p> <ul style="list-style-type: none"> <li>• Minimum length</li> <li>• Expiration interval</li> <li>• Complexity requirements</li> <li>• Invalid login attempt lockout threshold</li> </ul>	No exceptions noted.
5.22	User accounts are assigned to predefined access roles to restrict access to certain functions within the Alegeus application.	Inspected the user access listing and user groups to determine that user accounts were assigned to predefined access roles to restrict access to certain functions within the Alegeus application.	No exceptions noted.
5.23	User accounts are assigned to predefined access roles to restrict access to certain functions within the Content Central application.	Inspected the user access listing and user groups to determine that user accounts were assigned to predefined access roles to restrict access to certain functions within the Content Central application.	No exceptions noted.

**CONTROL AREA 5****INFORMATION SECURITY**

Control Objective Specified  
by the Service Organization:

Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

<b>Control Point</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
5.24	User accounts are assigned to predefined access roles to restrict access to certain functions within the ShoreTel application.	Inspected the user access listing and user groups to determine that user accounts were assigned to predefined access roles to restrict access to certain functions within the ShoreTel application.	No exceptions noted.
5.25	User accounts are assigned to predefined access roles to restrict access to certain functions within the TPA services application.	Inspected the user access listing and security profile definitions to determine that user accounts were assigned to predefined access roles to restrict access to certain functions within the TPA services application.	No exceptions noted.
5.26	User accounts are assigned to predefined access roles to restrict access to certain functions within the administration system application.	Inspected the user access listing and security profile definitions to determine that user accounts were assigned to predefined access roles to restrict access to certain functions within the administration system application.	No exceptions noted.

**CONTROL AREA 6****DATA COMMUNICATIONS**

Control Objective Specified by the Service Organization:

Control activities 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
6.1	A stateful inspection firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram and firewall rule set to determine that a stateful inspection firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
6.2	Administrative access within the firewall system is restricted to a user account accessible by CDN IT personnel.	<p>Inquired of the IT supervisor regarding firewall access to determine that administrative access within the firewall system was restricted to a user account accessible by CDN IT personnel.</p> <p>Inspected the firewall administrator listing to determine that administrative access within the firewall system was restricted to a single user account.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
6.3	An IPS is in place to monitor the production network for signatures recognized by the IPS.	Inspected the IPS configurations to determine that an IPS was in place to monitor the production network for signatures recognized by the IPS.	No exceptions noted.
6.5	Inbound Internet traffic terminates at a host in the demilitarized zone (DMZ) which is separate from the production network.	Inspected the network diagram to determine that inbound Internet traffic terminates at a host in the DMZ which was separate from the production network.	No exceptions noted.
6.6	Network address translation (NAT) is enabled on the firewall to translate internally routable IP addresses.	Inquired of the IT supervisor and CDN Partners third party network administrator to determine that NAT was enabled on the firewall to translate internally routable IP addresses.	No exceptions noted.

**CONTROL AREA 6**

**DATA COMMUNICATIONS**

Control Objective Specified by the Service Organization:

Control activities 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
6.7	Remote access to production environments is secured via encrypted VPN connections.	Inspected the listing of server IP addresses and the firewall rule set to determine that NAT was enabled on the firewall to translate internally routable IP addresses.	No exceptions noted.
6.8	The ability to remotely connect to production servers via a VPN connection is restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• President</li> <li>• Senior vice president of operations</li> <li>• Vice president of compliance and business development</li> <li>• Vice president of administration and finances</li> <li>• TPA Services Department Supervisor</li> <li>• IT department supervisor</li> <li>• HRA/FSA admin department supervisor</li> <li>• Plan Implementation &amp; Marketing Department Supervisor</li> <li>• Accounting Department Manager</li> <li>• Retirement Plan Administration Department Supervisor</li> </ul>	Inspected the VPN encryption configurations to determine that remote access to production environments was secured via encrypted VPN connections.	No exceptions noted.
	The ability to remotely connect to production servers via a VPN connection is restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• President</li> <li>• Senior vice president of operations</li> <li>• Vice president of compliance and business development</li> <li>• Vice president of administration and finances</li> <li>• TPA Services Department Supervisor</li> <li>• IT department supervisor</li> <li>• HRA/FSA admin department supervisor</li> <li>• Plan Implementation &amp; Marketing Department Supervisor</li> <li>• Accounting Department Manager</li> <li>• Retirement Plan Administration Department Supervisor</li> </ul>	Inspected the VPN configurations to determine that the ability to remotely connect to production servers via VPN connections was restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• President</li> <li>• Senior vice president of operations</li> <li>• Vice president of compliance and business development</li> <li>• Vice president of administration and finances</li> <li>• TPA Services Department Supervisor</li> <li>• IT department supervisor</li> <li>• HRA/FSA admin department supervisor</li> <li>• Plan Implementation &amp; Marketing Department Supervisor</li> </ul>	No exceptions noted.



**CONTROL AREA 6**

**DATA COMMUNICATIONS**

Control Objective Specified by the Service Organization:

Control activities 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
6.9	<ul style="list-style-type: none"> <li>• Accounting Department Supervisor</li> <li>• Quality Assurance Department Supervisor</li> <li>• Director of Compliance</li> <li>• Practiced Strategies</li> <li>• CNP Studios</li> <li>• Ademero</li> <li>• Envoy Plan Services</li> </ul> <p>The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall rule.</p>	<ul style="list-style-type: none"> <li>• Accounting Department Manager</li> <li>• Retirement Plan Administration Department Supervisor</li> <li>• Accounting Department Supervisor</li> <li>• Quality Assurance Department Supervisor</li> <li>• Director of Compliance</li> <li>• Practiced Strategies</li> <li>• CNP Studios</li> <li>• Ademero</li> <li>• Envoy Plan Services</li> </ul> <p>Inspected the firewall rule set to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall rule.</p>	No exceptions noted.

**CONTROL AREA 7****DATA ENTRY**

Control Objective Specified by the Service Organization:

Control activities provide reasonable assurance that data entry procedures are performed in an accurate and timely manner.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.1	The mail receiving clerk maintains a mail receiving log and enters the date contribution monies are received into a tracking spreadsheet.	<p>Inspected tracking spreadsheets for a sample of months during the review period to determine that contribution monies were logged into a tracking spreadsheet for each month sampled.</p> <p>Observed the mail receiving process to determine that the mail receiving clerk maintained a mail receiving log and entered the date contribution monies were received into a tracking spreadsheet.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
7.2	Contribution reports and monies are sent to the accounting department and recorded in a check log.	<p>Inquired of the Accounting Department Supervisor regarding contributions to determine that contribution reports and monies were sent to the accounting department and recorded in a check log.</p> <p>Inspected check logs for a sample of months during the review period to determine that contribution monies were recorded in a check log for each month sampled.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
7.3	The contribution monies recorded in the mail receiving clerk's tracking log and the accounting department's check log are reviewed by the accounting assistant on a monthly basis to ensure the amounts match.	Inquired of the Accounting Department Supervisor regarding the monthly reconciliation process to determine that the contribution monies recorded in the mail receiving clerk's tracking log and the accounting department's check log were reviewed by the accounting assistant on a monthly basis to ensure the amounts matched.	No exceptions noted.

**CONTROL AREA 7****DATA ENTRY**

Control Objective Specified  
by the Service Organization:

Control activities provide reasonable assurance that data entry procedures are performed in an accurate and timely manner.

<b>Control Point</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		Inspected the contribution money reconciliations for a sample of months during the review period to determine that the logs were reconciled for each month sampled.	No exceptions noted.

**CONTROL AREA 8**

**CONTRIBUTION PROCESSING**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that contribution amounts and monies received are posted to eligible participants' accounts in an accurate and timely manner.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
8.1	Contribution information is scanned into the system with a document imaging application and saved to a secure network drive for archiving and future retrieval of information.	<p>Inquired of a department supervisor regarding document imaging to determine that contribution information was scanned into a document imaging application and saved to a secured network drive for archiving and future retrieval of information.</p> <p>Inspected the access rights to the secured network drive where imaged contributions documents were stored to determine that contribution information was scanned into a document imaging application and saved to a secured network drive for archiving and future retrieval of information.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
8.2	Contribution information received from clients electronically is balanced in total to the check, wire, or ACH amount received.	<p>Inquired of the plan administration department supervisor to determine that contribution information received from clients electronically was balanced in total to the check, wire, or ACH amount received.</p> <p>Inspected the contribution reconciliation log for the review period and an example contribution checklist to determine that contribution information received from clients via electronic means was balanced in total to the check, wire, or ACH amount received.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
8.3	Documented contribution processing procedures are in place to guide personnel in the contributions processes.	Inspected the contribution processing procedures to determine that documented contribution procedures were in place.	No exceptions noted.

**CONTROL AREA 8**

**CONTRIBUTION PROCESSING**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that contribution amounts and monies received are posted to eligible participants' accounts in an accurate and timely manner.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
8.4	Enrollment information is entered into the administration system application from standard enrollment forms.	Inspected the standard enrollment forms to determine that enrollment information was entered into the administration system application from standard enrollment forms.	No exceptions noted.
8.5	Participant contribution information is imported into the administration system application. A member of the contribution processing department reviews the imported data in the administration application to ensure that it is correct and documents evidence of review in a peering spreadsheet.	<p>Inquired of the department supervisor regarding contribution information review to determine that participant contribution information was imported into the administration system application. A member of the contribution processing department reviewed the imported data in the administration application to ensure that it was correct and documented evidence of review in a peering spreadsheet.</p> <p>Inspected the peering spreadsheet log during the review period to determine that participant contribution information was imported into the administration system application. A member of the contribution processing department reviewed the imported data in the administration application to ensure that it was correct and documented evidence of review in a peering spreadsheet.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

**CONTROL AREA 9**

**CUSTOMER SERVICE**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that customer service activities are performed by trained personnel who are monitored for compliance with policies.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
9.1	Customer service management personnel silently monitor customer service calls for quality assurance purposes on a periodic basis. Call performance is formally assessed for each customer service representative ten times per month.	Observed the call performance reviews for a sample of customer service employees to determine that customer service management personnel silently monitored customer service calls for quality assurance purposes on a periodic basis. Call performance was formally assessed for each customer service representative ten times per month.	No exceptions noted.
9.2	Customer service personnel receive a formal review of their overall performance from management semi-annually.	Inspected the semi-annual reviews for a sample of customer service personnel to determine that customer service personnel received a formal review of their overall performance from management semi-annually.	No exceptions noted.
9.3	Customer service personnel undergo training to obtain knowledge of the various plan attributes.	<p>Inquired of the customer service department supervisor regarding training to determine that customer service personnel underwent training to obtain knowledge of the various plan attributes.</p> <p>Inspected the customer service personnel training courses scheduled and completed for a sample of customer service personnel hired during the review period to determine that the sampled customer service personnel underwent training of the various plan attributes.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

**CONTROL AREA 9****CUSTOMER SERVICE**

Control Objective Specified  
by the Service Organization:

Control activities provide reasonable assurance that customer service activities are performed by trained personnel who are monitored for compliance with policies.

<b>Control Point</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
9.4	Customer service personnel utilize automated call software to provide statistical analysis regarding customer service phone activity.	Inquired of the customer service department supervisor regarding call monitoring to determine that customer service personnel utilized automated call software to provide statistical analysis regarding customer service phone activity.  Observed an example of a recently generated automated call software statistical reports to determine that automated call software was in place to provide information on customer service phone activity.	No exceptions noted.  No exceptions noted.
9.5	Management meets to discuss customer service issues on a weekly basis.	Inspected the management meeting minutes for a sample of weeks during the review period to determine that management met to discuss customer service issues during each week sampled.	No exceptions noted.

**CONTROL AREA 10****DISTRIBUTION PROCESSING**

Control Objective Specified by the Service Organization:

Control activities provide reasonable assurance that distribution requests are entered and processed accurately and timely.

<b>Control Point</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
10.1	A check log is maintained that details the last check number used and the number of checks printed.	Inspected the check log for the review period to determine that a check log was maintained during the review period that detailed the last check number used and the number of checks printed.	No exceptions noted.
10.2	A checklist is created for each plan distribution run to guide administration and accounting personnel during the distribution process.	Inquired of the plan administration department supervisor regarding the distribution process to determine that a checklist was created for each plan distribution run to guide administration and accounting personnel during the distribution process.  Inspected the distribution checklist for a sample of distributions processed during the review period to determine that a checklist was created for each plan distribution run to guide administration and accounting personnel during the distribution process.	No exceptions noted.  No exceptions noted.
10.3	A password is required to print checks in the check printing application.	Inspected the check printing application authentication prompt to determine that a password was required to print checks in the check printing application.	No exceptions noted.



**CONTROL AREA 10****DISTRIBUTION PROCESSING**

Control Objective Specified by the Service Organization:

Control activities provide reasonable assurance that distribution requests are entered and processed accurately and timely.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
10.4	<p>A positive pay file is created and sent to the financial institution. The accounting assistant reviews daily notices from the third party financial institution that identifies possible fraudulent checks for a decision on whether or not to pay the check. Access to third party financial institution pay/return positive pay notifications is restricted to user accounts accessible by persons holding the following positions:</p> <ul style="list-style-type: none"> <li>• Vice president of administration and finance</li> <li>• Senior vice president of operations</li> <li>• Accounting supervisor</li> </ul>	<p>Inspected a fraudulent check positive pay file to determine that a positive pay file was created and sent to the financial institution and that the accounting team reviewed daily notices from the financial institution which identified possible fraudulent checks for a decision on whether or not to pay the check and that access to third-party financial institution pay/return positive pay notifications was restricted to user accounts accessible by persons holding the following positions:</p> <ul style="list-style-type: none"> <li>• Vice-president of administration and finance</li> <li>• Senior vice president of operations</li> <li>• Accounting supervisors</li> </ul>	No exceptions noted.
10.5	<p>Access to post the suppressed distribution requests in the administration system application is restricted to administration application user accounts accessible by persons holding the following positions:</p> <ul style="list-style-type: none"> <li>• Plan administrator</li> <li>• Distribution processors</li> </ul>	<p>Inspected the administration system user access listing to determine that access to post the suppressed distribution requests in the administration system application was restricted to administration application user accounts accessible by persons holding the following positions:</p> <ul style="list-style-type: none"> <li>• Plan administrator</li> <li>• Distribution processors</li> </ul>	No exceptions noted.

**CONTROL AREA 10**

**DISTRIBUTION PROCESSING**

Control Objective Specified by the Service Organization:

Control activities provide reasonable assurance that distribution requests are entered and processed accurately and timely.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
10.6	Access to print checks in the check printing application is restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• Senior vice president of operations</li> <li>• Vice president of administration and finance</li> <li>• Accounting department manager</li> <li>• Accounting department supervisor</li> <li>• Senior accounting assistant</li> </ul>	Inspected a listing of the check printing application users to determine that access to print checks in the check printing application was restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• Senior vice president of operations</li> <li>• Vice president of administration and finance</li> <li>• Accounting department manager</li> <li>• Accounting department supervisor</li> <li>• Senior accounting assistant</li> </ul>	No exceptions noted.
10.7	Accounting personnel review the detail of the check file loaded into the commercial check writing application to ensure that the format of the checks is correct and that the number of checks printed matches the number of checks listed on the distribution run checklist. The distribution checklist is initialed upon completion of this task.	Inquired of the plan administration department supervisor regarding the check file review process to determine that accounting personnel reviewed the detail of the check file loaded into the commercial check writing application to ensure that the format of the checks was correct and that the number of checks printed matched the number of checks listed on the distribution run checklist. The distribution checklist was initialed upon completion of this task.	No exceptions noted.

**CONTROL AREA 10****DISTRIBUTION PROCESSING**

Control Objective Specified by the Service Organization:

Control activities provide reasonable assurance that distribution requests are entered and processed accurately and timely.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the distribution checklist for a sample of distributions processed during the review period to determine that accounting personnel reviewed the detail of the check file loaded into the commercial check writing application to ensure that the format of the checks was correct and that the number of checks printed matched the number of checks listed on the distribution run checklist. The distribution checklist was initialed upon completion of this task.	No exceptions noted.
10.8	Distribution processors enter distribution request forms into the administration system application. The new requests are placed in a suppressed status.	Observed the data entry process with the plan administration department supervisor to determine that distribution processors entered distribution request forms into the administration system application and the new requests were placed in a suppressed status.	No exceptions noted.
10.9	Documented distribution procedures and schedules are in place to guide personnel in the distribution processes and date requirements.	Inspected the distribution procedures and schedules to determine that documented distribution procedures and schedules were in place to guide personnel in the distribution processes and date requirements.	No exceptions noted.
10.10	For Section 3121 and APPLE distribution requests, an approved distribution authorization report is required from the client before the distributions are posted in the administration application.	Inquired of the plan administration department supervisor regarding the distribution authorization report to determine that for Section 3121 and APPLE distribution requests, an approved distribution authorization report was required from the client before the distributions were posted in the administration application.	No exceptions noted.

**CONTROL AREA 10**

**DISTRIBUTION PROCESSING**

Control Objective Specified by the Service Organization:

Control activities provide reasonable assurance that distribution requests are entered and processed accurately and timely.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
10.11	Recurring Special Pay / HRA distributions are entered into a tracking spreadsheet to help ensure that the recurring payments are entered in the correct time period.	<p>Inspected the 3121 and Apple distribution authorization reports for a sample of clients and months within the review period to determine that for Section 3121 and APPLE distribution requests, an approved distribution authorization report was required from the client before the distributions were posted in the administration application.</p> <p>Inquired of the plan administration department supervisor regarding recurring payouts to determine that recurring Special Pay / HRA distributions were entered into a tracking spreadsheet to help ensure that the recurring payments were entered in the correct time period.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
10.12	The administration application is updated with the amount of the distribution, check number, and issue date. Completion of this task is recorded on the distribution checklist.	<p>Inspected the recurring distribution spreadsheet to determine that recurring Special Pay/HRA distributions were entered into a tracking spreadsheet to help ensure that the recurring payments were entered in the correct time period.</p> <p>Inquired of the plan administration department supervisor regarding the application update process to determine that the administration application was updated with the amount of the distribution, check number, and issue date.</p>	<p>No exceptions noted.</p>

**CONTROL AREA 10**

**DISTRIBUTION PROCESSING**

Control Objective Specified by the Service Organization:

Control activities provide reasonable assurance that distribution requests are entered and processed accurately and timely.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
10.13	The distribution processor verifies the number of distribution payments exported from the proprietary utility tool to the checklist created by administration personnel. The distribution checklist is initialed upon completion of this task.	<p>Inspected the distribution checklist for a sample of distributions processed during the review period to determine that the checklist was initialed to evidence that the administration application was updated with the distribution amount, check number, and issue date for each distribution sampled.</p> <p>Inquired of the plan administration department supervisor regarding the distribution payment count process to determine that the distribution processor verified the number of distribution payments exported from the proprietary utility tool to the checklist created by administration personnel.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
10.14	The mail receiving clerk date stamps distribution request forms received from the client. The forms are then forwarded to distribution processors.	<p>Inspected the distribution checklist for a sample of distributions processed during the review period to determine that the checklist was initialed to evidence that the distribution payment file count was verified for each distribution sampled.</p> <p>Inquired of the plan administration department supervisor regarding mail receiving to determine that the mail receiving clerk date stamped and forwarded each distribution request form to the distribution processors.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

**CONTROL AREA 10**

**DISTRIBUTION PROCESSING**

Control Objective Specified by the Service Organization:

Control activities provide reasonable assurance that distribution requests are entered and processed accurately and timely.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
10.15	The plan administrator compares the information entered into the administration system application to the distribution form to ensure that the information entered is correct and conforms to the distribution processing guidelines. The distribution checklist is initialed upon completion of this task.	<p>Inspected the distribution request forms for a sample of distributions processed during the review period to determine that the mail receiving clerk date stamped and forwarded each distribution request form to the distribution processors.</p> <p>Inquired of the plan administration department supervisor regarding distributions to determine that the plan administrator compared the information entered into the administration system application to the distribution form to ensure that the information entered was correct and conformed to the distribution processing guidelines.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
10.16	The plan administrator resolves errors in payee amounts which are identified on an error report, before check processing can continue.	<p>Inspected the distribution checklist for a sample of distributions processed during the review period to determine that the plan administrator compared the information entered into the administration system application to the distribution form to ensure that the information entered was correct and conformed to the distribution processing guidelines.</p> <p>Inquired of the plan administration department supervisor regarding error resolution to determine that the plan administrator resolved errors in payee amounts which were identified on an error report, before check processing continued.</p>	<p>No exceptions noted.</p>

**CONTROL AREA 10**

**DISTRIBUTION PROCESSING**

Control Objective Specified by the Service Organization:

Control activities provide reasonable assurance that distribution requests are entered and processed accurately and timely.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
10.17	The vice president of administration and finance or the accounting supervisor performs a final review of the printed checks to ensure that the total amount and the count of the printed checks match the amount that was previously approved. The distribution checklist is initialed upon completion of this task.	<p>Inspected an example recently generated error report to determine that the plan administrator resolved errors in payee amounts which were identified on an error report, before check processing continued.</p> <p>Inquired of the plan administration department supervisor regarding the final check review process to determine that the vice president of administration and finance or the accounting supervisor performed a final review of the printed checks to ensure that the total amount and the count of the printed checks matched the amount that was previously approved.</p> <p>Inspected the distribution checklist for a sample of distributions processed during the review period to determine that the checklist was initialed to evidence that the final check review was performed for each distribution sampled.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**CONTROL AREA 11****VALUATION**

Control Objective Specified  
by the Service Organization:

Control activities provide reasonable assurance that account valuation procedures are performed accurately.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
11.1	A gains basis and participants that have zero or less balance reports are produced on a monthly basis and provided to the team leads for review.	<p>Inquired of the plan administration department supervisor regarding the gains basis reports to determine that a gains basis and participants that had zero or less balance reports were produced on a monthly basis and provided to the team leads for review.</p> <p>Inspected the gains basis and participants that had zero or less gains reports for a sample of months within the review period to determine that a gains basis and participants that have zero or less gains reports were produced for each month sampled.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
11.2	A month end valuation checklist is utilized to guide plan administrators in completing month end valuation tasks.	Inspected the month end valuation checklist for a sample of months within the review period to determine that a month end valuation checklist was utilized to guide plan administrators in completing valuation tasks for each month sampled.	No exceptions noted.
11.3	A plan administrator reconciles the client's plan on the distribution partner's website to the administration system balance on a monthly basis.	Inquired of the accounting supervisor regarding the month end earnings reconciliation to determine that a plan administrator reconciled the client's plan on the distribution partner's website to the administration system balance on a monthly basis.	No exceptions noted.



**CONTROL AREA 11**

**VALUATION**

Control Objective Specified by the Service Organization:

Control activities provide reasonable assurance that account valuation procedures are performed accurately.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
11.4	Plan administrators reconcile the posted participant contributions and distributions to the trust statement on a monthly basis to determine the earnings or dividends that should be posted to the administration system. The month end valuation checklist is initialed upon completion of this task.	<p>Inspected reconciliation reports for a sample of months during the review period to determine that the client’s plan on the distribution partner’s website was reconciled to the administration system balance monthly.</p> <p>Inquired of the plan administration department supervisor regarding the trust statement reconciliation process to determine that plan administrators reconciled the posted participant contributions and distributions to the trust statement to determine the earnings or dividends that should be posted to the administration system.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
11.5	Reports to identify accounts with a negative balance as shown on the administration system application are produced on a monthly basis. The month end valuation checklist is initialed upon completion of this task.	<p>Inspected the month end valuation checklist for a sample of months within the review period to determine that the month end valuation checklist was initialed to evidence that contributions and distributions were reconciled to the trust statement for each month sampled.</p> <p>Inquired of the plan administration department supervisor regarding negative balance reports to determine that reports to identify accounts with a negative balance as shown on the administration system application were produced on a monthly basis.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

**CONTROL AREA 11**

**VALUATION**

Control Objective Specified  
by the Service Organization:

Control activities provide reasonable assurance that account valuation procedures are performed accurately.

<b>Control Point</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
11.6	The plan administrator reviews the administration checklist and supporting documentation, and signs the administration checklist as evidence of their review.	Inspected the month end valuation checklist for a sample of months during the review period to determine that reports to identify accounts with a negative balance as shown on the administration system application were produced on a monthly basis. The month end valuation checklist was initialed upon completion of this task.  Inspected the month end valuation checklist for a sample of months during the review period to determine that the team lead signed the administration checklist as evidence of their review for each month sampled.	No exceptions noted.  No exceptions noted.

**CONTROL AREA 12**

**PARTICIPANT STATEMENTS**

Control Objective Specified by the Service Organization:

Control activities provide reasonable assurance that participant statements are printed accurately and sent timely to participants.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
12.1	A log of the number of statements printed is created by the plan administrators and reviewed by the team lead to ensure that the correct number of statements was included in the PDF document sent to the mail clerk.	Inquired of the plan administration department supervisor regarding statement logs to determine that a log of the number of statements printed was created by the plan administrators and reviewed by the team lead to ensure that the correct number of statements was included in the PDF document sent to the mail clerk.  Inspected the statement log to determine that a log of the number of statements printed was created by the plan administrators and reviewed by the team lead to ensure that the correct number of statements was included in the PDF document sent to the mail clerk.	No exceptions noted.  No exceptions noted.
12.2	A statement schedule outlines when the statements are required to be printed and mailed for each plan.	Inspected the statement schedule to determine that a statement schedule outlined when the statements were required to be printed and mailed for each plan.	No exceptions noted.
12.3	Documented statement printing procedures are in place to guide plan administrators in participant statement printing process.	Inspected the participant statement instructions to determine that documented statement printing procedures were in place.	No exceptions noted.
12.4	Plan administrators compare administration system reports to ensure that statements include the correct balance information.	Inquired of the plan administration department supervisor regarding the participant statement totals to determine that plan administrators compared administration system reports to ensure that statements included the correct balance information.	No exceptions noted.

**CONTROL AREA 12**

**PARTICIPANT STATEMENTS**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that participant statements are printed accurately and sent timely to participants.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
12.5	The plan administrators compare a summary page of the printed statements to the valuation report to ensure that the information from the valuation report matches the PDF file of statements.	<p>Observed the participant statement review process with the administration plan department supervisor to determine that plan administrators compared administration system reports to ensure that statements included the correct balance information.</p> <p>Inquired of the plan administration department supervisor regarding the statement review process to determine that a summary page of the printed statements was compared to the valuation report by the plan administrators to ensure that the information from the valuation report matched the PDF file of statements.</p> <p>Inspected example statement reconciliation documentation to determine that the plan administrators compared a summary page of the printed statements to the valuation report to ensure that the information from the valuation report matched the PDF file of statements.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**CONTROL AREA 13**

**HRA CLAIMS PROCESSING**

Control Objective Specified by the Service Organization:

Control activities provide reasonable assurance that Health Reimbursement Account claims are adjudicated accurately and completely.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
13.1	Claims adjudicators are trained on the HRA claims adjudication and distribution process as a component of the hiring process.	<p>Inquired of the health and welfare department supervisor regarding training to determine that claims adjudicators were trained on the HRA claims adjudication and distribution process as a component of the hiring process.</p> <p>Inspected the standard claims adjudication training schedule and the individual training plan completion documents for a sample of new health and welfare adjudicators to determine that claims adjudicators were trained on the HRA claims adjudication and distribution process as a component of the hiring process.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
13.2	Documented procedures are in place to guide distribution personnel in the claims payment and review process.	Inspected the distribution policies and procedures to determine that documented procedures were in place to guide distribution personnel in the claims payment and review process.	No exceptions noted.
13.3	If a claim is denied, the claims adjudicator notifies the participant of the denial.	<p>Inquired of the health and welfare department supervisor regarding denied claims to determine that if a claim was denied, the claims adjudicator notified the participant of the denial.</p> <p>Inspected a sample of denial letters manually generated during the review period to determine that if the claim was denied, the claims adjudicator notified the participant of the denial.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

**CONTROL AREA 13**

**HRA CLAIMS PROCESSING**

Control Objective Specified by the Service Organization:

Control activities provide reasonable assurance that Health Reimbursement Account claims are adjudicated accurately and completely.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
13.4	If the claim is approved, the claim form is processed by a distribution processor who keys in the payee information and amount in administration system and stamps the form as "Entered" when complete.	<p>Inspected an example of an automatically generated denial letter to determine that if a claim was denied, the claims adjudicator notified the participant of the denial.</p> <p>Inquired of the health and welfare department supervisor regarding approved claims to determine that if the claim was approved, the claim form was processed by a distribution processor who keyed in the payee information and amount in administration system and stamps the form as "Entered" when complete.</p> <p>Inspected the claim form for a sample of approved HRA distributions processed during the review period to determine that if the claim was approved, the claim form was processed by a distribution processor who keys in the payee information and amount in administration system and stamps the form as "Entered" when complete.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
13.5	Reference materials are maintained to guide claims adjudicators in establishing the reimbursement eligibility of submitted claims.	Inspected the HRA claims reference and training materials to determine that reference materials were maintained to guide claims adjudicators in establishing the reimbursement eligibility of submitted claims.	No exceptions noted.

**CONTROL AREA 13**

**HRA CLAIMS PROCESSING**

Control Objective Specified by the Service Organization:

Control activities provide reasonable assurance that Health Reimbursement Account claims are adjudicated accurately and completely.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
13.6	The claims adjudicator reviews the claim to ensure the claim form is signed and the necessary information is included.	<p>Inquired of the health and welfare department supervisor regarding the claims process to determine that the claims adjudicator reviewed the claim to ensure the claim form was signed and the necessary information was included.</p> <p>Inspected a sample of claim request forms provided by the health and welfare department supervisor to determine that the claims adjudicator reviewed the claim to ensure the claim form was signed and the necessary information was included.</p> <p>Observed the claim review process with the health and welfare department supervisor to determine that the claims adjudicator reviewed the claim to ensure the claim form was signed and the necessary information was included.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**CONTROL AREA 14**

**TPA AND TPA SERVICES APPLICATION SERVICES**

Control Objective Specified by the Service Organization:

Control activities provide reasonable assurance that the 403(b) administration services including vendor oversight, plan administration and compliance, common remitting oversight and reporting are performed accurately and completely.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
14.1	402(g) and 415 compliance limits are monitored throughout the year for clients who submit payroll data for common remitting.	Observed the compliance monitoring process with the TPA services department supervisor to determine that 402(g) and 415 compliance limits were monitored throughout the year for clients who submitted payroll data for common remitting.	No exceptions noted.
14.2	A common remitting service is offered to clients that elect the service. Those clients are required to sign a common remitting service agreement.	<p>Inquired of the TPA services department supervisor regarding common remitting to determine that a common remitting service agreement was signed by each client that elected to use the common remitting services.</p> <p>Inspected the common remitting service agreement for a sample of new common remitting clients enrolled during the review period to determine that a common remitting service agreement was signed by each client that elected to use the common remitting services.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
14.3	A denial letter is sent to participants if their transaction request is denied.	<p>Inquired of the TPA services department supervisor regarding denial letters to determine that a denial letter was sent to participants when their transaction request was denied.</p> <p>Inspected a sample of denial letters provided by the TPA services department supervisor to determine that a denial letter was sent to participants when their transaction request was denied.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>



**CONTROL AREA 14**

**TPA AND TPA SERVICES APPLICATION SERVICES**

Control Objective Specified by the Service Organization:

Control activities provide reasonable assurance that the 403(b) administration services including vendor oversight, plan administration and compliance, common remitting oversight and reporting are performed accurately and completely.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
14.4	A plan document and a plan adoption agreement are prepared for the client as a component of the plan setup process.	<p>Inquired of the TPA services department supervisor regarding plan documents to determine that a plan document and a plan adoption agreement were prepared as a component of the client setup process.</p> <p>Inspected the plan adoption agreement for a sample of clients enrolled during the review period to determine that a plan adoption agreement was prepared for each client sampled.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
14.5	Adjudicators review participant transaction requests to ascertain whether the request is allowed by the plan. Adjudicators stamp the request cover sheet to indicate approval if the request is allowed by the plan.	<p>Inquired of the TPA services department supervisor regarding the adjudication process to determine that adjudicators reviewed participant transaction requests to ascertain whether the request was allowed by the plan. Adjudicators stamped the request cover sheet to indicate approval if the request was allowed by the plan.</p> <p>Observed the transaction request review process with the TPA services department supervisor to determine that adjudicators reviewed participant transaction requests to ascertain whether the request was allowed by the plan. Adjudicators stamped the request cover sheet to indicate approval if the request was allowed by the plan.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

**CONTROL AREA 14**

**TPA AND TPA SERVICES APPLICATION SERVICES**

Control Objective Specified by the Service Organization:

Control activities provide reasonable assurance that the 403(b) administration services including vendor oversight, plan administration and compliance, common remitting oversight and reporting are performed accurately and completely.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
14.6	An approved vendor list is prepared for the client as a component of the plan setup process.	Inspected the approved vendor list within the plan documents for a sample of new clients enrolled during the review period to determine that an approved vendor list was prepared for each client sampled.	No exceptions noted.
14.7	Approved vendors are required to sign an information sharing agreement (“ISA”.)	Inspected the ISA’s for a sample of new clients enrolled during the review period to determine that the approved vendors were required to sign an information sharing agreement.	No exceptions noted.
14.8	Documented policies and procedures are in place to guide personnel in the 403(b) administration process.	Inspected the policies and procedures to determine that documented policies and procedures were in place to guide personnel in the 403(b) administration process.	No exceptions noted.
14.9	SRA configuration changes in the TPA services application are placed in a pending status until they are reviewed and approved by 403(b) plan administration personnel.	<p>Inquired of the TPA services department supervisor regarding the SRA change process to determine that SRA configuration changes in the TPA services application were placed in a pending status until they were reviewed and approved by 403(b) plan administration personnel.</p> <p>Observed the SRA entry process with the TPA services department supervisor to determine that SRA configuration changes in the TPA services application were placed in a pending status until they were reviewed and approved by 403(b) plan administration personnel.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

**CONTROL AREA 14**

**TPA AND TPA SERVICES APPLICATION SERVICES**

Control Objective Specified by the Service Organization:

Control activities provide reasonable assurance that the 403(b) administration services including vendor oversight, plan administration and compliance, common remitting oversight and reporting are performed accurately and completely.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
14.10	SRAs are assigned to vendors based on the information on the SRA form. The TPA services application is configured with a pre-populated listing of approved vendors.	<p>Inspected the TPA services application configurations to determine that SRAs were assigned to vendors based on the information on the SRA form and the TPA services application was configured with a pre-populated listing of approved vendors.</p> <p>Observed the SRA entry process with the TPA services department supervisor to determine that SRAs were assigned to vendors based on the information on the SRA form.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
14.11	The 403(b) plan administration manager or team supervisor finalizes payroll files in a “releasable” status, which archives contributions in plan and participant records in the TPA services application.	Observed the common remitting process with the TPA services department supervisor to determine that the 403(b) plan administration manager or team supervisor finalized payroll files in a “releasable” status, which archived contributions in plan and participant records in the TPA services application.	No exceptions noted.
14.12	The 403(b) plan administration manager or team supervisor reconciles finalized payroll files to the funds received by accounting on a daily basis. Evidence of the reconciliation is recorded on a common remitting checklist.	Inspected the common remitting distribution checklists and the accounting log for a sample of days during the review period to determine that the 403(b) plan administration manager or team supervisor reconciled finalized payroll files to the funds received by accounting and recorded completion of the reconciliation on a common remitting checklist each day.	No exceptions noted.

**CONTROL AREA 14**

**TPA AND TPA SERVICES APPLICATION SERVICES**

Control Objective Specified by the Service Organization:

Control activities provide reasonable assurance that the 403(b) administration services including vendor oversight, plan administration and compliance, common remitting oversight and reporting are performed accurately and completely.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
14.13	The TPA services application reconciles payroll information received from the client to the expected amount in the TPA services application. Any variances or issues are resolved by 403(b) personnel before the payroll can be processed.	<p>Inquired of the TPA services department supervisor regarding the common remitting process to determine that the TPA services application reconciled payroll information received from the client to the expected amount in the TPA services application, and that any variances or issues were resolved by 403(b) personnel before the payment can be processed.</p> <p>Observed the common remitting process with the TPA services department supervisor to determine that the TPA services application reconciled payroll information received from the client to the expected amount in the TPA services application, and that any variances or issues were resolved by 403(b) personnel before the payment can be processed.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

**CONTROL AREA 15****CLIENT IMPLEMENTATION**

Control Objective Specified by the Service Organization:

Controls provide reasonable assurance that new/conversion plan provisions, account balances and investment elections are accurately recorded in Relius.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
15.1	Each new plan is peer-reviewed after it has been set up to verify that all steps required to complete the implementation of a plan have been performed.	Inspected the status log and the related peer-reviewer's initials for the population of new plans to determine that each new plan is peer-reviewed after it has been set up to verify that all steps required to complete the implementation of a plan had been performed.	No exceptions noted.
15.2	Procedures are in place for the new plan setup and peer review process.	Inspected the procedures for setting up new plan implementations to determine that procedures were in place for the new plan setup and peer review process.	No exceptions noted.
15.3	The compliance department verifies that the plan document has the appropriate signatures.	Inspected the status log for the population of new plans to determine that the compliance department verified that the plan document had the appropriate signatures.	No exceptions noted.
15.4	The compliance department verifies that the plan highlights have been approved.	Inspected the status log for the population of new plans to determine that the compliance department verified that the plan highlights had been approved.	No exceptions noted.
15.5	The implementation team sets up and the compliance department reviews the plan specifications in Relius for accuracy.	Inspected the status log for the population of new plans to determine that the implementation team sets up the new plans and the compliance department reviewed the plan specifications in Relius for accuracy.	No exceptions noted.

**CONTROL AREA 15****CLIENT IMPLEMENTATION**

Control Objective Specified by the Service Organization:

Controls provide reasonable assurance that new/conversion plan provisions, account balances and investment elections are accurately recorded in Relius.

<b>Control Point</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
15.6	The peer review process requires the completion of a comprehensive checklist covering the areas of documentation, Relius setup, Relius VRU and web setup, contact management and communications.	Inspected the peer review checklist to determine that the peer review process required the completion of a comprehensive checklist covering the areas of documentation, Relius setup, Relius VRU and web setup, contact management and communications.	No exceptions noted.

**SECTION 6**  
**OTHER INFORMATION PROVIDED**  
**BY THE SERVICE ORGANIZATION**

## **DISASTER RECOVERY PLANNING**

MidAmerica has implemented control activities to provide reasonable assurance that policies and procedures are in place to minimize disruption of processing activities and services to user entities in the event of a business interruption or natural disaster. Specific processes that MidAmerica has implemented in this area are described below:

- A disaster recovery plan has been implemented to guide personnel in the performance of disaster recovery procedures
- The disaster recovery plan is tested periodically
- An agreement is maintained for a remote hot site to restore business operations in the event of an extended business interruption or natural disaster