A-LIGN

MidAmerica Administrative & Retirement Solutions, Inc.
Type 2 SOC 1
2019

MidAmerica

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

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

October 1, 2018 to September 30, 2019

Table of Contents

SECTION 1 ASSERTION OF MIDAMERICA ADMINISTRATIVE & RETIREMENT SOLUTIONS, INC.'S MANAGEMENT 1

SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT 4

SECTION 3 DESCRIPTION OF MIDAMERICA ADMINISTRATIVE & RETIREMENT SOLUTIONS, INC.'S PLAN ADMINISTRATION SERVICES SYSTEM 8

OVERVIEW OF OPERATIONS 9
Company Background 9
Description of Services Provided 9
Boundaries of the System 12
Subservice Organizations 12
Significant Changes in the Last 12 Months 13
CONTROL ENVIRONMENT 13
Integrity and Ethical Values 13
Commitment to Competence 14
Management's Philosophy and Operating Style 14
Organizational Structure and Assignment of Authority and Responsibility 14
Human Resources Policies and Practices 15
RISK ASSESSMENT 15
CONTROL OBJECTIVE AND RELATED CONTROL ACTIVITIES 16
Integration with Risk Assessment 16
MONITORING 16
On-Going Monitoring 16
INFORMATION AND COMMUNICATION SYSTEMS 17
Information Systems 17
Communication Systems 18
COMPLEMENTARY USER ENTITY CONTROLS 18

SECTION 4 DESCRIPTION OF MIDAMERICA ADMINISTRATIVE & RETIREMENT SOLUTIONS, INC.'S CONTROL OBJECTIVES AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS 20

GUIDANCE REGARDING DESCRIPTION OF MIDAMERICA ADMINISTRATIVE & RETIREMENT SOLUTIONS, INC.'S CONTROL OBJECTIVES AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS 21
PHYSICAL SECURITY 22
COMPUTER OPERATIONS - BACKUP 25
COMPUTER OPERATIONS - AVAILABILITY 26
INFORMATION SECURITY 28
DATA COMMUNICATIONS 40
DATA ENTRY 42
CONTRIBUTION PROCESSING 44
CUSTOMER SERVICE 46
VALUATION 49
PARTICIPANT STATEMENTS 51
HRA CLAIMS PROCESSING 53
CLIENT IMPLEMENTATION 55

SECTION 1

ASSERTION OF MIDAMERICA ADMINISTRATIVE & RETIREMENT SOLUTIONS, INC.'S MANAGEMENT

MidAmerica

Assertion of MidAmerica Administrative & Retirement Solutions, Inc.'s Management

November 30, 2019

We have prepared the description of MidAmerica Administrative & Retirement Solutions, Inc.'s ('MidAmerica' or 'the Company') Plan Administration Services system for processing user entities' transactions entitled "Description of MidAmerica Administrative & Retirement Solutions, Inc.'s Plan Administration Services System" throughout the period October 1, 2018 to September 30, 2019, (description) for user entities of the system during some or all of the period October 1, 2018 to September 30, 2019, and their user auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

MidAmerica uses Corserva, Inc. ('Corserva' or 'subservice organization') for data center hosting. The description includes only the control objectives and related controls of MidAmerica and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by MidAmerica in the description can be achieved only if complementary subservice organization controls assumed in the design of MidAmerica's controls are suitably designed and operating effectively, along with the related controls at MidAmerica. The description does not extend to controls of the subservice organization.

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

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

a. The description fairly presents the Plan Administration Services system made available to user entities of the system during some or all of the period October 1, 2018 to September 30, 2019, for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

   i. presents how the system made available to user entities of the system was designed and implemented to process relevant 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) services performed by a subservice organization, if any, including whether the inclusive method or the carve-out method has been used in relation to them.

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

(8) 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. includes relevant details of changes to the service organization's system during the period covered by the description.

iii. 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 controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period October 1, 2018 to September 30, 2019, to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of MidAmerica's controls throughout the period October 1, 2018 to September 30, 2019. 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.

Jim Tormey
President and CEO
MidAmerica Administrative &
Retirement Solutions, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To MidAmerica Administrative & Retirement Solutions, Inc.:

Scope

We have examined MidAmerica Administrative & Retirement Solutions, Inc.'s ('MidAmerica' or 'the Company') description of its Plan Administration Services system for processing user entities' transactions entitled "Description of MidAmerica Administrative & Retirement Solutions, Inc.'s Plan Administration Services System" throughout the period October 1, 2018 to September 30, 2019, (description) and the suitability of the design and operating effectiveness of MidAmerica's controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Assertion of MidAmerica Administrative & Retirement Solutions, Inc.'s Management" (assertion).

MidAmerica uses Corserva, Inc. ('Corserva' or 'subservice organization') for data center hosting. The description includes only the control objectives and related controls of MidAmerica and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by MidAmerica can be achieved only if complementary subservice organization controls assumed in the design of MidAmerica are suitably designed and operating effectively, along with the related controls at MidAmerica. Our examination did not extend to controls of the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design and operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In Section 1 of this report, MidAmerica has provided their assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. MidAmerica is responsible for preparing the description and their assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

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

We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period October 1, 2018 to September 30, 2019. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

Inherent Limitations

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

Description of Tests of Controls

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

Opinion

In our opinion, in all material respects, based on the criteria described in MidAmerica's assertion,

a. the description fairly presents the Plan Administration Services system that was designed and implemented throughout the period October 1, 2018 to September 30, 2019.
b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2018 to September 30, 2019 and subservice organizations and user entities applied the complementary user entity controls contemplated in the design of MidAmerica's controls throughout the period October 1, 2018 to September 30, 2019.
c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period October 1, 2018 to September 30, 2019, if complementary subservice organization and user entity controls assume in the design of MidAmerica's controls operated effectively throughout the period October 1, 2018 to September 30, 2019.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4 is intended solely for the information and use of MidAmerica, user entities of MidAmerica's Plan Administration Services system during some or all of the period October 1, 2018 to September 30, 2019, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

A-LIGN ASSURANCE

November 30, 2019
Tampa, Florida

SECTION 3

DESCRIPTION OF MIDAMERICA ADMINISTRATIVE & RETIREMENT SOLUTIONS, INC.'S PLAN ADMINISTRATION SERVICES SYSTEM

OVERVIEW OF OPERATIONS

Company Background

MidAmerica Administrative and Retirement Solutions, LLC ("MARS") provides benefits funding and administration solutions for public sector employers focusing on education and government markets. MARS is a provider of Social Security Alternative and Special Pay plans, HRAs, FSAs, 403(b)s and GASB Trusts products serving over one million employees and 2,700 sponsors across the country.

Description of Services Provided

Health Reimbursement Arrangement

MARS' single largest product segment is the Health Reimbursement Arrangement ('HRA'), commonly referred to as a health reimbursement account, an employer-funded, tax-advantaged health benefit plan that reimburses employees for out-of-pocket medical expenses and individual health insurance premiums. The employer and employee both save 7.65% in FICA taxes (Social Security and Medicare). Funds carry over year-to-year. Deposits, accumulation, and reimbursements are tax-free. Employers customize Plan (iHRA, dcHRA or rHRA) options including contribution type and frequency, eligibility, vesting, reimbursements, and forfeiture provisions, which creates a competitive benefits package to attract and retain talent. Funds are invested and grow tax-free with a guaranteed minimum rate of return. Variable options are also available.

Special Pay Plan

A Special Pay Plan is an employer-funded, defined contribution retirement plan for full-time employees. Funded upon retirement or separation of service, 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. This retirement plan is designed to handle special forms of compensation in a tax-advantaged manner by allowing employers and employees to save 7.65% FICA taxes (Social Security and Medicare) contributions while also deferring income tax for the employee. Funds are invested in a fixed or variable investment account, which may increase account value due to earnings over time and may be self-directed to meet personal retirement goals. The Plan is governed by IRS Section 403(b) or 401(a) guidelines.

Social Security Alternative Plan

A Social Security Alternative Plan, commonly referred as 3121 FICA Alternative Plan or A.P.P.L.E. Plan, is, typically, an employee-funded qualified savings plan designed as an alternative to Social Security that allows part-time, temporary, and seasonal employees of government entities to contribute 7.5% of their before-tax wages to an investment account. Employers save the matching 6.2% Social Security contribution, replacing it with an impactful benefit for employees. Funds are invested in a fixed or variable investment account, which may increase the account value due to earnings over time and may be self-directed to meet personal retirement goals. The Plan is governed by IRS Section 457(b), 401(a) or 403(b) guidelines.

Employer Sponsored Plan

The Employer Sponsored Plan is an employer-funded, defined contribution retirement plan for full-time employees. Similar to a Special Pay Plan, the plan is funded using unique forms of compensation such as unused sick leave and unused vacation pay while the employee is actively working (no access to funds until retirement) rather than in full at retirement, providing a benefit that grows during employment. Funds are deposited into a 403(b) or 401(a) retirement plan in a tax-advantaged manner by allowing employers and employees to save 7.65% FICA taxes (Social Security and Medicare) on employer contributions while also deferring income tax for the employee.

Flexible plan design allows the employer to attach a vesting schedule to control participant eligibility. Funds are invested and grow tax-free with a guaranteed minimum rate of return. Variable options are also available.

Employee Benefit Trust

Many employers provide Other Post-Employment Benefits ('OPEB') such as continuing health care coverage for their employees after retirement. These benefits oftentimes must be paid out of the employer's current operational budget leaving employers vulnerable to a large OPEB liability. Additionally, the GASB, through Statement 4, requires the disclosure of this liability on financial statements. Disclosure of this liability, absent an offsetting asset, can significantly impact the employer's financial statements, adversely affecting the credit rating. An OPEB Trust allows the employer to set aside money to fund future liabilities while the employee is actively working, minimizing the impact of these liabilities. Funds are invested, which means assets grow over time.

Physical Security

MidAmerica's main office is in Lakeland, FL, located at 2855 Interstate Drive, Suite 115. Physical access to MidAmerica's offices is controlled by card reader security systems. All doors that provide access to the 115 Suite are locked at all times. Access cards are assigned to MidAmerica staff and other authorized individuals. Visitors to the Interstate Dr. office must gain entry to the office through the reception area, where they are asked to sign a log and wear a visitor badge if they will be entering the office beyond reception area.

The creation and management of access cards for the offices is handled by the MidAmerica Lakeland Office Manager. A quarterly review of active badges for both security systems is performed by the Lakeland Office Manager to ensure that badges have appropriate access levels, and badges that have been misplaced or were assigned to terminated employees are inactive.

Each security system has the following access levels for the card reader entry system:

1. Master/24-7 Access - Senior management, IT Department Supervisor, Tenants & Building Owners, Cleaners.
2. Supervisor/Extended Staff - Weekday and weekend access during business hours for Supervisors and IT staff.
3. Staff - Weekday access during business hours for staff and vendors.

The in-scope system and supporting infrastructure is hosted by Corserva. As such, Corserva is responsible for the physical security controls for the in-scope system.

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 MidAmerica personnel in real time via e-mail. Once alerted, the MidAmerica personnel 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. 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 an Oracle database. Administrative access to the application is restricted to authorized personnel.

The Relius administration application requires 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.

Data Communications

A Fortinet firewall is in place to restrict traffic to the network. Specific firewall rules are configured to allow certain services, ports and protocols while denying traffic not specifically allowed. Network address translation is configured to translate internally routable IP addresses via “friendly” host object names. Administrators manage 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.

Transactions Processing & Reporting

Data Entry

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

Significant Events

MidAmerica has implemented automated and manual procedures to capture and address significant events and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with detailed information that impacts the 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
- Information Technology (‘IT’) Team - manages, monitors, and supports internal information systems
- Accounting Team - responsible for processing distribution checks and performing reconciliations related to services provided to user entities. Also provides financial and regulatory reporting and compliance

- 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
- Participant Services Team - responsible for answering inbound calls from program participants

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 does not include the data center hosting services provided by Corserva at the Orlando, Florida facility.

Subservice Description of Services

MidAmerica utilizes Corserva to manage a portion of their technology services, including data center hosting, basic IT support services, such as patch releases and antivirus updates, and server monitoring management and support. Corserva also provides disaster recovery services for all datacenter hosted devices.

Complementary Subservice Organization Controls

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

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

Subservice Organization - Corserva	
Control Objective	**Control**
Computer Operations - Backup	Corserva performs daily incremental backups (Sunday-Friday) of all key corporate intellectual property and other business data using a cloud-based service. Full backups occur on Saturday. Restore tests are performed.
Computer Operations - Availability	Corserva personnel monitor hosted client systems for system alerts and outages and notify client personnel.
	Monitoring solutions/tools are deployed on the application and network to monitor availability, health, and capacity metrics, including planned maintenance on the Windows environment. The tools are configured to send alerts to IT Operations based on predefined thresholds where they are analyzed and remediated.
	Corserva utilizes uninterruptible power supplies, gasoline and natural gas powered backup generators to ensure availability during a power outage or emergency. Fire Suppression and FM200 systems are in place. There is redundant power and ISP providers in place.

Subservice Organization - Corserva	
Control Objective	**Control**
	Corserva performs daily incremental backups (Sunday-Friday) of all key corporate intellectual property and other business data using a cloud-based service. Full backups occur on Saturday. Restore tests are performed.
	Business continuity and recovery procedures are documented in a Business Continuity Plan, and tested on an annual basis.
Physical Security	Appropriate security controls are in place to prevent unauthorized physical access to the servers within the Corserva's Data Centers.
	All visitors must provide and surrender a government issued picture ID (e.g. Driver's License) and have had access rights granted prior to their visit. Each Visitor is logged into Corserva's database upon entry along with any equipment that is entering or exiting the facility.
	All secondary exits are alarmed and monitored with closed caption television system.
	All entrances/exits are monitored with surveillance cameras. Additional video surveillance, as well as biometrics entry and motion detection devices, is implemented within the colocation space separated by hardened walls from standard Customer and staff access space.
	Corserva servers and Customer computer, network and related equipment is contained in a secure cage within the Data Center.

MidAmerica management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant control objectives through written contracts, such as service level agreements. In addition, MidAmerica performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by Corserva
- Holding periodic discussions with vendors and subservice organization
- Making regular site visits to vendor and subservice organization facilities
- Testing controls performed by vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

Significant Changes in the Last 12 Months

MidAmerica moved into a new facility in the Lakeland area in the Spring of 2019. This allowed for not only the upgrade of the overall office environment, but an upgrade to office-based infrastructure equipment to ensure the organization was prepped for scalability into the future. Additionally, our servers were moved to an offsite location in Orlando.

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 comply
- Policies and procedures require employees to sign an acknowledgment form indicating 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 the service organization has implemented in this area are:

- 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

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 the service organization has implemented in this area are:

- 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:

- 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 an annual basis thereafter
- Customer service representatives receive monthly 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 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 has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of those objectives.

Selection and Development of Control Activities Specified by the Service Organization

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

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, adjacent to the service organization's description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

MONITORING

Management monitors controls to ensure 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:

- Quarterly review of badge access assignments for accuracy
- Monitoring of IT infrastructure issues and incidents

- Regular customer service call monitoring and evaluations
- Periodic customer service satisfaction surveys
- Performance of daily and monthly reconciliations throughout the plan administration process

Vendor Management

MidAmerica has defined the following activities to oversee controls performed by vendors that could impact the Plan Administration system:

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and subservice organization
- Making regular site visits to vendor and subservice organization facilities
- Testing controls performed by vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

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 DL360	Virtualization layer of the Network running on VMWare vSphere 6.5.
Storage Area Network ('SAN')	HP StoreVirtual 4730	Storage for the Virtual Hosts and Shares.
Wireless	Cisco Meraki	Guest network with WPA2 security. Internal network access via WPA2 Enterprise security utilizing Microsoft Active Directory.

Software

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

Primary Software	
Software	**Purpose**
Alegeus	Administration system for HSA and HRA plans.
MARS Utilities	Developed internally, the software is used to pull information from Relius to create direct deposit and check files.
Relius	Administration system that houses the majority of the client data, with the exception of the plans hosted in Alegeus and Relevant Remitter.
Onbase by Hyland	Enterprise content management system to index, store, and route files.

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

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

Control Area 5: Information Security

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 immediately notifying MidAmerica of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

Control Area 7: Data Entry

4. User entities are responsible for ensuring that data submitted to MidAmerica is complete, accurate and timely.
5. User entities are responsible for ensuring their data are formatted in accordance with agreed upon standards.

Control Area 8: Contribution Processing

6. User entities are responsible for submitting contribution payments in an accurate and timely manner.

Control Areal 10: Distribution Processing

7. User entities are responsible for reviewing and approving the distribution authorization lists sent by MidAmerica.
8. User entities are responsible for reviewing distribution request forms for completeness before they are sent to MidAmerica.

SECTION 4

DESCRIPTION OF MIDAMERICA ADMINISTRATIVE & RETIREMENT SOLUTIONS, INC.'S CONTROL OBJECTIVES AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

GUIDANCE REGARDING DESCRIPTION OF MIDAMERICA ADMINISTRATIVE & RETIREMENT SOLUTIONS, INC.'S CONTROL OBJECTIVES AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

A-LIGN's examination of the controls of MidAmerica was limited to the control objectives and related control activities specified by the management of MidAmerica and did not encompass all aspects of MidAmerica's operations or operations at user organizations. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No. 18 (SSAE 18).

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

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

In determining whether a SSAE 18 report meets the user auditor's objectives, the user auditor should perform the following procedures:

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

CONTROL AREA 1 **PHYSICAL SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that physical access to system data and functions is properly authorized and administered.

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.	Observed the exterior office entrances to determine that a badge access system was in place to restrict access to the office.	No exceptions noted.
1.2	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 in place to guide personnel in determining access rights.	No exceptions noted.
1.3	A receptionist monitors and controls access to the office during normal business hours.	Observed the office entrance to determine that a receptionist monitored and controlled access to the office during normal business hours.	No exceptions noted.
1.4	Administrative access within the badge access system is restricted to user accounts accessible by persons holding the following positions: • Vice President ('VP') of Information Technology ('IT') • IT Consultant • Office Manager	Inquired of the IT consultant regarding badge access administrators to determine that administrative access within the badge access system was restricted to user accounts accessible by persons holding the following positions: • VP of IT • IT Consultant • Office Manager	No exceptions noted.
		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: • VP of IT • IT Supervisor • Office Manager	No exceptions noted.
1.5	Badge access is revoked as a component of the termination process.	Inquired of the IT consultant regarding the access revocation process to determine that badge access was revoked as a component of the termination process.	No exceptions noted.

CONTROL AREA 1 **PHYSICAL SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that physical access to system data and functions is properly authorized and administered.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the termination notification incident ticket and badge access listing for a sample of terminated employees terminated during the review period to determine that badge access was revoked as a component of the termination process.	No exceptions noted.
1.6	Exterior doors to the office are locked at all times.	Inquired of the IT consultant regarding office security to determine that exterior doors to the office were locked at all times.	No exceptions noted.
		Observed the office entrances to determine that exterior doors to the office were locked during business hours.	No exceptions noted.
1.7	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.
1.8	The office manager reviews badge access permissions on a quarterly basis to help ensure that badge access permissions are authorized for each employee.	Inquired of the IT consultant regarding the badge access review process to determine that the office manager reviewed badge access permissions on a quarterly basis to help ensure that badge access permissions were authorized for each employee.	No exceptions noted.
		Inspected the badge access review documentation for a sample of quarters during the review period to determine that the office manager reviewed badge access permissions on a quarterly basis to help ensure that badge access permissions were authorized for each employee.	No exceptions noted.

CONTROL AREA 1 **PHYSICAL SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that physical access to system data and functions is properly authorized and administered.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.9	Visitors are required to sign a visitors' log upon entering the office suite.	Inquired of the IT consultant regarding visitor logs to determine that visitors were required to sign a visitors' log upon entering the office.	No exceptions noted.
		Observed the visitor access process to determine that visitors were required to sign a visitor's log upon entering the office suite.	No exceptions noted.
		Inspected visitor logs for a sample of months during the review period to determine that visitors were required to sign a visitor's log upon entering the office suite.	No exceptions noted.

CONTROL AREA 2 **COMPUTER OPERATIONS - BACKUP**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that timely system backups of critical files to an off-site location are performed.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.1	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.
2.2	IT personnel utilize an automated backup system to perform incremental backups of production data on a daily basis, Sunday through Saturday.	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 incremental backups of production data on a daily basis, Sunday through Saturday.	No exceptions noted.
2.3	The automated backup system is configured to replicate backup data to a third-party data center.	Inspected third-party data center SSAE 18, service level agreement, and replication configurations to determine that the automated backup system was configured to replicate backup data to a third-party data center.	No exceptions noted.
2.4	The automated backup system is configured to send backup completion status e-mail notifications to IT personnel.	Inspected the automated backup system notification configurations to determine that the automated backup system was configured to send backup completion status e-mail notifications to IT personnel.	No exceptions noted.
2.5	Backups of sensitive client information are encrypted.	Inspected the backup encryption policy to determine that backups of sensitive client information were encrypted.	No exceptions noted.

CONTROL AREA 3 **COMPUTER OPERATIONS - AVAILABILITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that system processing is authorized and executed in a complete, accurate, and timely manner, and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete accurate and timely manner.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.1	An enterprise monitoring application is configured to send e-mail notifications of production outages to 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 IT personnel.	No exceptions noted.
3.2	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.
3.3	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 plan to determine that documented incident response policies and procedures were in place to guide personnel in reporting and responding to major information technology incidents.	No exceptions noted.
3.4	A disaster recovery plan is in place to guide employees in the event of significant unplanned incidents.	Inspected the disaster recovery procedures to determine that a disaster recovery plan was in place to guide employees in the event of significant unplanned incidents.	No exceptions noted.
3.5	Tests of the disaster recovery plan are performed semi-annually to ensure the operating effectiveness of the disaster recovery plan.	Inspected the disaster recovery plan test results to determine that tests of the disaster recovery plan were performed semi-annually to ensure the operating effectiveness of the disaster recovery plan.	No exceptions noted.
3.6	IT personnel log operational issues into a ticketing system and assign personnel to monitor the status of the issues.	Inquired of the IT Consultant 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.

CONTROL AREA 3 **COMPUTER OPERATIONS - AVAILABILITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that system processing is authorized and executed in a complete, accurate, and timely manner, and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete accurate and timely manner.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected a sample of incident tickets to determine that operational issues were logged into a ticketing system and assigned personnel to monitor the status of the issues.	No exceptions noted.

CONTROL AREA 4 **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
4.1	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.
4.2	The network domain is configured to enforce the following password requirements: • Password history • Password age (minimum & maximum) • Password Length • Complexity • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the network password and account lockout configurations to determine that the network domain was configured to enforce the following password requirements: • Password history • Password age (minimum & maximum) • Password Length • Complexity • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
4.3	Administrative access within the network domain is restricted to user accounts accessible by persons holding the following positions: • Vice President ('VP') of Information Technology ('IT') • IT Team Leader • Infrastructure Analyst • IT Project Manager • IT Project Manager • Senior Program Analyst • IT Consultant	Inquired of the IT Consultant, regarding network admin privileges to determine that administrative access within the network domain was restricted to user accounts accessible by persons holding the following positions: • VP of IT • IT Team Leader • Infrastructure Analyst • IT Project Manager • IT Project Manager • Senior Program Analyst • IT Consultant	No exceptions noted.

CONTROL AREA 4 **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 network administrator listing to determine that administrative access within the network domain was restricted to user accounts accessible by persons holding the following positions: • VP of IT • IT Team Leader • Infrastructure Analyst • IT Project Manager • IT Project Manager • Senior Program Analyst • IT Consultant	No exceptions noted.
4.4	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 sample of terminated employees to determine that access to the network domain was revoked as a component of the termination process.	No exceptions noted.

CONTROL AREA 4 **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
	Web and Database Server Operating System Access		
4.5	Administrative access within the web and database server operating systems is restricted to user accounts accessible by personnel holding the following positions: • VP of IT • IT Team Leader • Infrastructure Analyst • IT Project Manager • IT Project Manager • Senior Program Analyst • IT Consultant	Inquired of the IT Consultant regarding server administrative access to determine that administrative access within the web and database servers was restricted to user accounts accessible by personnel holding the following positions: • VP of IT • IT Team Leader • Infrastructure Analyst • IT Project Manager • IT Project Manager • Senior Program Analyst • IT Consultant	No exceptions noted.
		Inspected the server operating system administrator listing to determine that administrative access within the web and database servers was restricted to user accounts accessible by personnel holding the following positions: • VP of IT • IT Team Leader • Infrastructure Analyst • IT Project Manager • IT Project Manager • Senior Program Analyst • IT Consultant	No exceptions noted.

CONTROL AREA 4 **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
	SQL Database Authentication and Access		
4.6	Administrative access within the database is restricted to user accounts accessible by personnel holding the following positions: • IT Team Leader • IT Project Manager	Inquired of the IT Consultant regarding database administrative privileges to determine that administrative access within the database was restricted to user accounts accessible by personnel holding the following positions: • IT Team Leader - April Brown • IT Project Manager - Charles Connors	No exceptions noted.
		Inspected the listing of user accounts with administrative access to the database and their roles and privileges to determine that administrative access within the database was restricted to a shared user account accessible by persons holding the following positions: • IT Team Leader • IT Project Manager	No exceptions noted.
	Oracle Database Authentication and Access		
4.7	Users are required to authenticate via a user account and password before being granted access to the database.	Inquired of the IT Consultant regarding database administrative privileges to determine that users were required to authenticate via a user account and password before being granted access to the database.	No exceptions noted.
		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.

CONTROL AREA 4 **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
4.8	Administrative access within the database is restricted to default user accounts accessible by persons holding the following positions: • VP of IT • IT Team Leader • Infrastructure Analyst • IT Project Manager • IT Project Manager • Senior Program Analyst • IT Consultant	Inquired of the IT Consultant, regarding database access to determine that administrative access within the database was restricted to default user accounts accessible by persons holding the following positions: • VP of IT • IT Team Leader • Infrastructure Analyst • IT Project Manager • IT Project Manager • Senior Program Analyst • IT Consultant	No exceptions noted.
		Inspected the domain administrative user listing and the oracle database roles to determine that administrative access within the database was restricted to default user accounts accessible by persons holding the following positions: • VP of IT • IT Team Leader • Infrastructure Analyst • IT Project Manager • IT Project Manager • Senior Program Analyst • IT Consultant	No exceptions noted.

CONTROL AREA 4 **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
	Application Level Authentication and Access		
4.9	Relius application users are required to authenticate via a user account and password before being granted access to the administration system application.	Inspected the Relius authentication configurations to determine that Relius application users were required to authenticate via a user account and password before being granted access to the administration application.	No exceptions noted.
4.10	The Relius administration system application is configured to enforce the following password requirements: • Password Age Maximum • Password Length • Complexity	Inspected the Relius password configurations to determine that the Relius administration system application was configured to enforce the following password requirements: • Password Age Maximum • Password Length • Complexity	No exceptions noted.
4.11	User accounts are assigned to predefined access roles to restrict access to certain functions within the Relius administration system application.	Inspected the user access listing to determine that user accounts were assigned to predefined access roles to restrict access to certain functions within the Relius administration system application.	No exceptions noted.
4.12	Administrative access within the Relius administration application is restricted to user accounts accessible by persons holding the following access roles: • System Administrator • Team Leader with System Admin	Inquired of the IT Consultant regarding Relius admin access to determine that administrative access within the administration application was restricted to user accounts accessible by persons holding the following access roles: • System Administrator • Team Leader with System Admin	No exceptions noted.

CONTROL AREA 4 **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 Relius administration application user accounts to determine that administrative access within the administration application was restricted to user accounts accessible by persons holding the following access roles: • System Administrator • Team Leader with System Admin	No exceptions noted.
4.13	Access to the Relius administration system application is revoked as a component of the termination process.	Inquired of the IT Consultant regarding access revocation to determine that access to the administration system application was revoked as a component of the termination process.	No exceptions noted.
		Inspected the termination checklist and administration system application user account listing for a sample of terminated employees to determine that access to the administration system application was revoked as a component of the termination process.	No exceptions noted.
4.14	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.
4.15	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.

CONTROL AREA 4 **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
4.16	Complete Administrative access within the Alegeus application is restricted to user accounts accessible by personnel holding the following positions: • IT Team Leader • Infrastructure Analyst • Senior Program Analyst • IT Consultant	Inquired of the IT Consultant regarding application admin access to determine that complete administrative access within the Alegeus application was restricted to user accounts accessible by personnel holding the following positions: • IT Team Leader • Infrastructure Analyst • Senior Program Analyst • IT Consultant	No exceptions noted.
		Inspected the listing of Alegeus application administrator accounts to determine that complete administrative access within the Alegeus application was restricted to user accounts accessible by personnel holding the following positions: • IT Team Leader • Infrastructure Analyst • Senior Program Analyst • IT Consultant	No exceptions noted.
4.17	Access to the Alegeus application is revoked as a component of the termination process.	Inquired of the IT Consultant, regarding access revocation to determine that access to the Alegeus application was revoked as a component of the termination process.	No exceptions noted.
		Inspected the termination checklist and the Alegeus application user account listing for a sample of terminated employees to determine that access to the Alegeus application was revoked as a component of the termination process.	No exceptions noted.

CONTROL AREA 4 **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
4.18	Application users are required to authenticate via username and password before being granted access to the OnBase application.	Inspected the OnBase password configurations to determine that application users were required to authenticate via username and password before being granted access to the OnBase application.	No exceptions noted.
4.19	User accounts are assigned to predefined access roles to restrict access to certain functions within the OnBase 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 OnBase application.	No exceptions noted.
4.20	Administrative access within the OnBase application is restricted to user accounts accessible by personnel holding the following positions: • IT Consultant • IT Team Leader • IT Project Manager • Infrastructure Analyst • Senior Program Analyst	Inquired of the IT Consultant, Bob Pascucci, regarding application administrative access to determine that administrative access within the OnBase application was restricted to user accounts accessible by personnel holding the following positions: • IT Consultant • IT Team Leader • IT Project Manager • Infrastructure Analyst • Senior Program Analyst	No exceptions noted.

CONTROL AREA 4 **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 OnBase application administrator accounts to determine that administrative access within the OnBase application was restricted to user accounts accessible by personnel holding the following positions: • IT Consultant • IT Team Leader • IT Project Manager • Infrastructure Analyst • Senior Program Analyst	No exceptions noted.
4.21	Access to the OnBase application is revoked as a component of the termination process.	Inquired of the IT Consultant regarding access revocation to determine that access to the OnBase application was revoked as a component of the termination process.	No exceptions noted.
		Inspected the termination checklist and OnBase application user account listing for a sample of terminated employees to determine that access to the OnBase application was revoked as a component of the termination process.	No exceptions noted.
4.22	Application users are required to authenticate via a password before being granted access to the BroadSmart application.	Inspected the application authentication configurations to determine that application users were required to authenticate via a password before being granted access to the BroadSmart application.	No exceptions noted.
4.23	User accounts are assigned to predefined access roles to restrict access to certain functions within the BroadSmart 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 BroadSmart application.	No exceptions noted.

CONTROL AREA 4 **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
4.24	Administrative access within the BroadSmart application is restricted to user accounts accessible by personnel holding the following positions: • Vice President of IT • IT Consultant • IT Team Leader • IT Project Manager • Infrastructure Analyst	Inquired of the IT Consultant regarding application administrative access to determine that administrative access within the BroadSmart application was restricted to user accounts accessible by personnel holding the following positions: • Vice President of IT • IT Consultant • IT Team Leader • IT Project Manager • Infrastructure Analyst	No exceptions noted.
		Inspected the listing of BroadSmart application administrator accounts to determine that administrative access within the BroadSmart application was restricted to user accounts accessible by personnel holding the following positions: • Vice President of IT • IT Consultant • IT Team Leader • IT Project Manager • Infrastructure Analyst	No exceptions noted.
4.25	Access to the BroadSmart application is revoked as a component of the termination process.	Inquired of the IT Consultant regarding BroadSmart access to determine that access to the BroadSmart application was revoked as a component of the termination process.	No exceptions noted.

CONTROL AREA 4 **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 termination checklist and BroadSmart application user account listing for a sample of terminated employees to determine that access to the BroadSmart application was revoked as a component of the termination process.	No exceptions noted.

CONTROL AREA 5 **DATA COMMUNICATIONS**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that data transmissions between the service organization and its clients are complete, accurate, and secure and that data received is posted to the relevant systems in accordance with the Company's guidelines.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.1	A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
5.2	Administrative access within the firewall system is restricted to user accounts accessible by personnel holding the following positions: • Vice President of IT • IT Consultant • Infrastructure Analyst	Inquired of the IT Consultant regarding firewall administrative access to determine that administrative access within the firewall system was restricted to user accounts accessible by personnel holding the following positions: • Vice President of IT • IT Consultant • Infrastructure Analyst	No exceptions noted.
		Inspected the firewall administrator listing to determine that administrative access within the firewall system was restricted to user accounts accessible by personnel holding the following positions: • Vice President of IT • IT Consultant • Infrastructure Analyst	No exceptions noted.
5.3	An intrusion prevention system ('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.
5.4	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.

CONTROL AREA 5 **DATA COMMUNICATIONS**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that data transmissions between the service organization and its clients are complete, accurate, and secure and that data received is posted to the relevant systems in accordance with the Company's guidelines.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.5	Network address translation ('NAT') is enabled on the firewall to translate internally routable IP addresses.	Inquired of the IT Consultant, regarding information security methods and tool configurations to determine that NAT was enabled on the firewall to translate internally routable IP addresses.	No exceptions noted.
		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.
5.6	Remote access to production environments is secured via encrypted virtual private network ('VPN') connections.	Inspected the VPN configurations to determine that remote access to production environments was secured via encrypted VPN connections.	No exceptions noted.
5.7	The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall rule.	Inspected the firewall ruleset to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall rule.	No exceptions noted.
5.8	The online document upload portal that clients and plan participants use to send files to MidAmerica is encrypted via secure socket layer ('SSL').	Inspected the SSL digital certificate to determine that the online document upload portal that clients and plan participants used to send files to MidAmerica was encrypted via SSL.	No exceptions noted.

CONTROL AREA 6 **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
6.1	The mail receiving clerk scans the contribution monies received into the OnBase database.	Observed the mail receiving process to determine that the mail receiving clerk scanned the contribution monies received into the OnBase database.	No exceptions noted.
6.2	The mail receiving clerk enters the date contribution monies are received into the OnBase database.	Observed the mail receiving process to determine that the mail receiving clerk entered the date contribution monies were received into the OnBase database.	No exceptions noted.
		Inspected the tracking spreadsheet and extracted OnBase log for the review period to determine that the mail receiving clerk entered the date contribution monies were received into the OnBase database.	No exceptions noted.
6.3	Contribution reports and funds are sent to the accounting department and recorded in a check log.	Inquired of the Finance and Accounting Manager regarding contributions to determine that contribution reports and funds were sent to the accounting department and recorded in a check log.	No exceptions noted.
		Inspected the check logs for a sample of months during the review period to determine that contribution reports and funds were sent to the accounting department and recorded in a check log.	No exceptions noted.
6.4	The contribution funds recorded in the mail receiving clerk's tracking log and the accounting department's check log are reviewed by the staff accounting assistant on a monthly basis to ensure the amounts match.	Inquired of the Finance and Accounting Manager regarding the monthly reconciliation process to determine that the contribution funds recorded in the mail receiving clerk's tracking log and the accounting department's check log were reviewed by the staff accounting assistant on a monthly basis to ensure the amounts matched.	No exceptions noted.

CONTROL AREA 6 **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
		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 7 **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
7.1	Documented contribution processing procedures are in place to guide personnel in the contributions process.	Inspected the contribution processing procedures to determine that documented contribution processing procedures were in place to guide personnel in the contributions process.	No exceptions noted.
7.2	Electronic contribution information received from clients is saved to a secure network drive for archiving and future retrieval of information.	Inquired of the Contributions Operations Manager regarding document imaging to determine that electronic contribution information received from clients was saved to a secured network drive for archiving and future retrieval of information.	No exceptions noted.
		Inspected the access rights to determine that electronic contribution information received from clients was saved to a secured network drive for archiving and future retrieval of information.	No exceptions noted.
7.3	Contribution information received from clients electronically is balanced in total to the check, wire, or automated clearing house ('ACH') amount received.	Inquired of the Contributions Operations Manager regarding contribution reception and balancing to determine that contribution information received from clients electronically was balanced in total to the check, wire, or ACH amount received.	No exceptions noted.
		Inspected the contribution reconciliation log for the review period to determine that contribution information received from clients via electronic means was balanced in total to the check, wire, or ACH amount received.	No exceptions noted.
7.4	Enrollment information is entered into the administration system application from standard enrollment forms.	Inspected a sample of standard enrollment forms to determine that enrollment information was entered into the administration system application from standard enrollment forms.	No exceptions noted.

CONTROL AREA 7 **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
7.5	Participant contribution information is imported into the administration system application by contributions processors. The senior contributions processor reviews the imported data for accuracy and sends an approval e-mail to the accounting department containing the daily list of contributions that are to be traded.	Inquired of the Contributions Operations Manager regarding contribution information importation to determine that participant contribution information was imported into the administration system application by contributions processors, and that the senior contributions processor reviewed the imported data for accuracy and sent an approval e-mail to the accounting department containing the daily list of contributions that were to be traded.	No exceptions noted.
		Inspected the approved contributions e-mail for a nonstatistical sample of days to determine that participant contribution information was imported into the administration system application by contributions processors, and that the senior contributions processor reviewed the imported data for accuracy and sent an approval e-mail to the accounting department containing the daily list of contributions that were to be traded.	No exceptions noted.

CONTROL AREA 8 **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
8.1	Customer service management personnel silently monitor customer service calls for quality assurance purposes on a periodic basis.	Inquired of the Participant Services Manager regarding call monitoring and Quality Assurance ('QA') practices to determine that customer service management personnel silently monitored customer service calls for quality assurance purposes on a periodic basis.	No exceptions noted.
		Observed the call performance review process to determine that customer service management personnel silently monitored customer service calls for quality assurance purposes on a periodic basis.	No exceptions noted.
8.2	Customer service personnel receive a formal review of their overall performance from management annually.	Inspected performance reviews for a sample of customer service personnel to determine that customer service personnel received a formal review of their overall performance from management annually.	No exceptions noted.
8.3	New customer service personnel receive a formal 90-day review of their overall performance.	Inspected the 90-day performance reviews for a sample of new employees to determine that new customer service personnel receive a formal 90-day review of their overall performance.	No exceptions noted.
8.4	Customer service personnel undergo training to obtain knowledge of the various plan attributes.	Inquired of the Participant Services Manager regarding new hire training to determine that customer service personnel underwent training to obtain knowledge of the various plan attributes.	No exceptions noted.
		Inspected the standardized training program and an example specialized training program to determine that customer service personnel underwent training to obtain knowledge of the various plan attributes.	No exceptions noted.

CONTROL AREA 8 **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
		Inspected the customer service personnel training courses scheduled and completed for a sample of customer service personnel hired to determine that the sampled customer service personnel underwent training of the various plan attributes.	Testing of this control activity disclosed that no customer service personnel hiring had occurred during the audit period.
8.5	Customer service personnel utilize automated call software to provide statistical analysis regarding customer service phone activity.	Inquired of the Participant Services Manager regarding call monitoring regarding call monitoring to determine that customer service personnel utilized automated call software to provide statistical analysis regarding customer service phone activity.	No exceptions noted.
		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.
8.6	Customer service personnel go through both general and specialized training to better suit the needs of the customer.	Inquired of the Participant Services Manager regarding call monitoring regarding call monitoring to determine that customer service personnel go through both general and specialized training to better suit the needs of the customer.	No exceptions noted.
		Inspected the standardized training program and an example specialized training program to determine that customer service personnel go through both general and specialized training to better suit the needs of the customer.	No exceptions noted.
8.7	Customer service personnel perform cross training to reduce wait time and better suit the needs of the customer.	Inquired of the Participant Services Manager regarding cross training practices to determine that customer service personnel perform cross training to reduce wait time and better suit the needs of the customer.	No exceptions noted.

CONTROL AREA 8 **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
		Inspected cross training request memo to determine that customer service personnel perform cross training to reduce wait time and better suit the needs of the customer.	No exceptions noted.
8.8	Quality assurance ('QA') compiles monthly call monitoring reports to evaluate performance and identify gaps in service.	Inquired of the Participant Services Manager regarding QA practices to determine that QA compiled monthly call monitoring reports to evaluate performance and identify gaps in service.	No exceptions noted.
		Inspected the QA call report for a sample of months to determine that QA compiled monthly call monitoring reports to evaluate performance and identify gaps in service.	No exceptions noted.
8.9	Customer service personnel receives a buddy and perform job shadowing as part of the specialized discipline training.	Inquired of the Participant Services Manager regarding training practices to determine that customer service personnel received a buddy and performed job shadowing as part of the specialized discipline training.	No exceptions noted.
		Inspected the standardized training program and an example specialized training program to determine that customer service personnel received a buddy and performed job shadowing as part of the specialized discipline training.	No exceptions noted.
		Inspected the buddy and job shadowing schedule for a sample of customer service personnel to determine that customer service personnel received a buddy and performed job shadowing as part of the specialized discipline training.	Testing of this control activity disclosed that no customer service personnel hiring had occurred during the audit period.

CONTROL AREA 9 **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
9.1	A gains basis report is produced on a monthly basis and provided to the team leads for review.	Inquired of the Invested Plans Team Leader regarding the gains basis reports to determine that a gains basis report was produced on a monthly basis and provided to the team leads for review.	No exceptions noted.
		Inspected the gains basis reports for a sample of months within the review period to determine that a gains basis report was produced on a monthly basis and provided to the team leads for review.	No exceptions noted.
9.2	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.
9.3	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.	Inquired of the Manager of Plan Administration regarding the trust statement reconciliation process to determine that plan administrators reconciled 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 and that the month end valuation checklist was initialed upon completion of this task.	No exceptions noted.

CONTROL AREA 9 **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
		Inspected the reconciliation documentation and the month end valuation checklist for a sample of months within the review period to determine that plan administrators reconciled 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 and that the month end valuation checklist was initialed upon completion of this task.	No exceptions noted.
9.4	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.	Inquired of the Manager of Plan Administration 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 and that the month end valuation checklist was initialed upon completion of this task.	No exceptions noted.
		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 and that the month end valuation checklist was initialed upon completion of this task.	No exceptions noted.
9.5	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 the plan administrator reviewed the administration checklist and supporting documentation and signed the administration checklist as evidence of their review.	No exceptions noted.

CONTROL AREA 10 **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
10.1	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 Document Manager Team Leader 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.	No exceptions noted.
		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.
10.2	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.
10.3	Documented statement printing procedures are in place to guide plan administrators in participant statement printing process.	Inspected the statement peering and HRA annual and quarterly statement instructions to determine that documented statement printing procedures were in place to guide plan administrators in participant statement printing process.	No exceptions noted.
10.4	Plan administrators compare administration system reports to ensure that statements include the correct balance information.	Inquired of the Manager of Plan Administration 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 10 **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
		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.	No exceptions noted.
10.5	The plan administrators compare a summary page of the printed statements for Relius HRA accounts to the valuation report to ensure that the information from the valuation report matches the PDF file of statements.	Inquired of the Manager of Plan Administration regarding the statement review process to determine that the plan administrators compared a summary page of the printed statements for Relius HRA accounts to the valuation report to ensure that the information from the valuation report matched the PDF file of statements.	No exceptions noted.
		Inspected the statement reconciliation documentation for a sample of Relius HRA clients to determine that the plan administrators compared a summary page of the printed statements for Relius HRA accounts to the valuation report to ensure that the information from the valuation report matched the PDF file of statements.	No exceptions noted.

CONTROL AREA 11 **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
11.1	Claims adjudicators are trained on the Health Reimbursement Arrangement ('HRA') claims adjudication and distribution process as a component of the hiring process.	Inquired of the HRA Manager regarding training to determine that claims adjudicators were trained on the HRA claims adjudication and distribution process as a component of the hiring process.	No exceptions noted.
		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.	No exceptions noted.
11.2	Documented procedures are in place to guide distribution personnel in the claims payment and review process.	Inspected the claims processing procedure and procedures to determine that documented procedures were in place to guide distribution personnel in the claims payment and review process.	No exceptions noted.
11.3	Reference materials are maintained to guide claims adjudicators in establishing the reimbursement eligibility of submitted claims.	Inquired of the HRA Manager regarding reference materials to determine that reference materials were maintained to guide claims adjudicators in establishing the reimbursement eligibility of submitted claims.	No exceptions noted.
		Observed the HRA claims reference and training materials on the company intranet to determine that reference materials were maintained to guide claims adjudicators in establishing the reimbursement eligibility of submitted claims.	No exceptions noted.
		Inspected the HRA claims reference and training materials and the entity's intranet to determine that reference materials were maintained to guide claims adjudicators in establishing the reimbursement eligibility of submitted claims.	No exceptions noted.

CONTROL AREA 11 **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
11.4	If a claim is denied, the claims adjudicator notifies the participant of the denial.	Inquired of the HRA Manager regarding denied claims to determine that if a claim was denied, the claims adjudicator notified the participant of the denial.	No exceptions noted.
		Inspected a sample of denial letters generated during the review period to determine that if the claim was denied, the claims adjudicator notified the participant of the denial.	No exceptions noted.
11.5	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 changes the status to “approved”.	Inquired of the HRA Manager 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 changed the status to “approved”.	No exceptions noted.
		Observed the claims approval process 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 changed the status to “approved”.	No exceptions noted.
11.6	The claims adjudicator reviews the claim to ensure the claim form is signed and the necessary information is included.	Inquired of the HRA Manager 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.	No exceptions noted.
		Observed the claim review process with the Health and Welfare Team Leader to determine that the claims adjudicator reviewed the claim to ensure the claim form was signed and the necessary information was included.	No exceptions noted.

CONTROL AREA 12 **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
12.1	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 was peer-reviewed after it had been set up to verify that all steps required to complete the implementation of a plan had been performed.	No exceptions noted.
12.2	Documented procedures are in place to guide personnel in the new plan setup and peer review processes.	Inspected the procedures for setting up new plan implementations to determine that documented procedures were in place to guide personnel in the new plan setup and peer review processes.	No exceptions noted.
12.3	The account management team verifies that the plan document has the appropriate signatures.	Inspected the status log for the population of new plans to determine that the account management team verified that the plan document had the appropriate signatures.	No exceptions noted.
12.4	The account management team verifies that the plan highlights have been approved.	Inspected the status log for the population of new plans to determine that the account management team verified that the plan highlights had been approved.	No exceptions noted.
12.5	The account management team sets up and the client implementation reviews the plan specifications in Relius for accuracy.	Inspected the status log for the population of new plans to determine that the account management team set up and the client implementation reviewed the plan specifications in Relius for accuracy.	No exceptions noted.
12.6	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 for a sample of clients implemented during the review period 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.