



# MidAmerica

Administrative & Retirement Solutions, Inc.

**MIDAMERICA ADMINISTRATIVE & RETIREMENT SOLUTIONS, INC.  
& SUBSIDIARIES**

PLAN ADMINISTRATION SERVICES

INDEPENDENT SERVICE AUDITOR'S REPORT ON A DESCRIPTION OF A SERVICE  
ORGANIZATION'S SYSTEM AND THE SUITABILITY OF THE DESIGN AND  
OPERATING EFFECTIVENESS OF CONTROLS

OCTOBER 1, 2012, TO SEPTEMBER 30, 2013

Attestation and Compliance Services



## BRIGHTLINE

Certified Public Accountants & Associates

Proprietary & Confidential

Unauthorized use, reproduction or distribution of this report, in whole or in part, is strictly prohibited.

This report is intended solely for use by the management of MidAmerica Administrative & Retirement Solutions, Inc. & Subsidiaries, its user entities (i.e., customers) that utilized the services covered by this report during the specified time period, and the independent financial statement auditors of those user entities (each referred to herein as a “specified user”).

If report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against BrightLine CPAs & Associates, Inc. as a result of such access. Further, BrightLine CPAs & Associates, Inc. does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction or distribution of this report, in whole or in part, is strictly prohibited.

# TABLE OF CONTENTS

SECTION 1	INDEPENDENT SERVICE AUDITOR'S REPORT .....	1
SECTION 2	MANAGEMENT'S AND SUBSERVICE ORGANIZATION'S ASSERTIONS .....	4
SECTION 3	DESCRIPTION OF MIDAMERICA'S SYSTEM AND ASPECTS OF CDN'S SYSTEM .....	8
SECTION 4	TESTING MATRICES .....	23
SECTION 5	OTHER INFORMATION PROVIDED BY MANAGEMENT .....	56

# **SECTION I**

## **INDEPENDENT SERVICE AUDITOR'S REPORT**

## INDEPENDENT SERVICE AUDITOR'S REPORT

To MidAmerica Administrative & Retirement Solutions, Inc. & Subsidiaries:

We have examined MidAmerica Administrative & Retirement Solutions, Inc. & Subsidiaries' ("MidAmerica" or the "service organization") description of its plan administration services system for processing user entities' transactions performed at the Lakeland, Florida, facility and CDN Partners, Inc.'s ("CDN" or the "subservice organization") description of relevant aspects of its network administration and support services throughout the period October 1, 2012, to September 30, 2013 (the "description"), and the suitability of the design and operating effectiveness of MidAmerica's and CDN's controls to achieve the related control objectives stated in the description. CDN is an independent service organization that provides network administration and support services to MidAmerica. MidAmerica's description includes a description of CDN's network administration and support services used by MidAmerica to process transactions for its user entities, as well as relevant control objectives and controls of CDN. 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 and CDN's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

In Section 2, MidAmerica and CDN have provided their assertions about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. MidAmerica and CDN are responsible for preparing the description and the assertions, including the completeness, accuracy, and method of presentation of the description and the assertions, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period October 1, 2012, to September 30, 2013.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and subservice organization and described in their respective assertions in Section 2. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Because of their nature, controls at a service organization or subservice organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization or subservice organization may become inadequate or fail.

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

- a. the description fairly presents MidAmerica's plan administration services system and CDN's network administration and support services used by MidAmerica to process transactions for its user entities that were designed and implemented throughout the period October 1, 2012, to September 30, 2013;
- b. the controls related to the control objectives of MidAmerica and CDN stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2012, to September 30, 2013, and user entities applied the complementary user entity controls contemplated in the design of MidAmerica's controls throughout the period October 1, 2012, to September 30, 2013; and
- c. the controls of MidAmerica and CDN that we tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period October 1, 2012, to September 30, 2013.

The specific controls tested and the nature, timing, and results of those tests are listed in Section 4 (the "Testing Matrices").

In Section 5, MidAmerica has provided additional information that is not a part of MidAmerica's description. Such information has not been subjected to the procedures applied in our examination of the description and of the suitability of design and operating effectiveness of controls to achieve the related control objectives stated in the description, and accordingly, we express no opinion on it.

This report, including the description of the tests of controls and results thereof in the Testing Matrices, is intended solely for the information and use of user entities of MidAmerica's plan administration services system during some or all of the period October 1, 2012, to September 30, 2013, 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.



Tampa, Florida  
November 4, 2013

## **SECTION 2**

### **MANAGEMENT'S AND SUBSERVICE ORGANIZATION'S ASSERTIONS**

## MANAGEMENT'S ASSERTION

We have prepared the description of MidAmerica Administrative & Retirement Solutions, Inc. & Subsidiaries' ("MidAmerica") plan administration services system (the "description") for user entities of the system during some or all of the period October 1, 2012, to September 30, 2013, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

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

- a. the description fairly presents the plan administration services system made available to user entities of the system during some or all of the period October 1, 2012, to September 30, 2013, for processing their transactions. MidAmerica uses CDN Partners, Inc. ("CDN") for aspects of MidAmerica's network administration and support services. The description in Section 3 includes both the controls and related control objectives of MidAmerica and the control objectives and related controls of CDN. The criteria we used in making our 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, as applicable:
    - (1) the types of services provided including, as appropriate, the classes of transactions processed;
    - (2) the procedures, within both automated and manual systems, by which services are provided, including, as appropriate, procedures by which transactions are authorized, recorded, processed, corrected as necessary, and transferred to reports and other information presented to user entities of the system;
    - (3) the related accounting records, supporting information, and specific accounts that are used to 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 of the system;
    - (4) how the system captures and addresses significant events and conditions, other than transactions;
    - (5) the process used to prepare reports or other information provided for entities of the system;
    - (6) specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls contemplated in the design of our controls; and
    - (7) other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.
  - ii. does not omit or distort information relevant to the scope of the plan administration services system, while acknowledging that the description is presented to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the plan administration services system that each individual user entity of the system and its user auditor may consider important in its own particular environment.
  - iii. The description includes relevant details of changes to the plan administration services system during the period October 1, 2012, to September 30, 2013.
- b. the controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period October 1, 2012, to September 30, 2013, to achieve those control objectives. The criteria we used in making this assertion were that



- i. the risks that threaten the achievement of the control objectives stated in the description have been identified by management;
- ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and
- iii. the controls were consistently applied as designed, and manual controls were applied by individuals who have the appropriate competence and authority.

## CDN'S ASSERTION

We have prepared the description of aspects of CDN Partners, Inc.'s ("CDN") network administration and support services system for MidAmerica Administrative & Retirement Solutions, Inc. & Subsidiaries ("MidAmerica") and user entities of MidAmerica's plan administration services system (the "description") for user entities of the system during some or all of the period October 1, 2012, to September 30, 2013, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

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

- a. the description fairly presents the aspects of CDN's network administration and support services system (the "system") made available to MidAmerica and user entities of MidAmerica's plan administration services system during some or all of the period October 1, 2012, to September 30, 2013, for processing their transactions. The criteria we used in making our assertion were that the description
  - i. presents how the system made available to MidAmerica and user entities of MidAmerica's plan administration services system was designed and implemented to process relevant transactions, including, as applicable:
    - (1) the types of services provided;
    - (2) how the system captures and addresses significant events and conditions, other than transactions;
    - (3) the process used to prepare reports or other information provided to MidAmerica;
    - (4) specified control objectives and controls designed to achieve those objectives; and
    - (5) other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.
  - ii. does not omit or distort information relevant to the scope of the relevant aspects of CDN's network administration and support services system made available to MidAmerica and user entities of MidAmerica's plan administration services system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the systems and their financial statement auditors, and may not, therefore, include every aspect of the plan administration services system that each individual user entity of the system and its auditor may consider important in its own particular environment.
  - iii. The description includes relevant details of changes to the relevant aspects of CDN's network administration and support services system made available to MidAmerica and user entities of MidAmerica's plan administration services system during Review Period October 1, 2012, to September 30, 2013.
- b. the controls related to the control objectives stated in the description that relate to the relevant aspects of CDN's network administration and support services system made available to MidAmerica were suitably designed and operating effectively throughout Review Period October 1, 2012, to September 30, 2013, to achieve those control objectives. The criteria we used in making this assertion were that
  - i. we have identified the risks that threaten the achievement of the control objectives stated in the description;
  - 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.

# SECTION 3

## DESCRIPTION OF MIDAMERICA'S SYSTEM AND ASPECTS OF CDN'S SYSTEM

---

## OVERVIEW OF OPERATIONS

### Company Background

MidAmerica Administrative & Retirement Solutions, Inc. & Subsidiaries (MidAmerica) provides employee benefit programs to 1,500 plan sponsors and over a half million employees across the country. Originally formed in 1995, MidAmerica focused primarily on providing Internal Revenue Code Section 3121 Social Security opt-out programs to governmental employers. The core business has grown and has expanded to include Health Reimbursement Arrangement, Health Savings Account and Flexible Spending Account administration, Special Pay programs, Governmental Accounting Standards Board (GASB) 45 programs, and more recently, independent 403(b) and 457 third party administration and common remitting services.

### Description of Services Provided

*The following is a brief description of the MidAmerica service lines:*

#### Health Reimbursement Arrangement (HRA)

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

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

#### Flexible Spending Account (FSA)

FSA, oftentimes called Section 125 Cafeteria plans, were formally created by Internal Revenue Code 125 of the Revenue Act of 1978. The Act allowed employees to set aside money on a pre-tax basis to pay for certain expenses. Expenses eligible for reimbursement include required employee contributions to an employer sponsored health care plan, dependent care expenses and any health care expenses not covered by the employer health care plan. Examples of these expenses include co-payments, deductibles, prescription drug purchases, eyeglasses and dental expenses or any other eligible uncovered medical expenses. Money deposited in FSA's must be used in the year it is deposited or the remaining balance is forfeited.

#### Special Pay Plan

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

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

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

#### Employer Sponsored 403(b) Plan

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

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

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

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

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

#### Employee Benefit Trust

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

#### Functional Areas of Operations

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

- Executive management – responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives
- IT department – manages, monitors, and supports internal information systems with the support of the third party vendor, CDN
- Accounting department – responsible for processing distribution checks and performing reconciliations related to services provided to user entities and provides financial and regulatory reporting and compliance
- 403(b) TPA team – responsible for vendor oversight, plan administration, and compliance monitoring
- Contribution processing team – responsible for the processing of contributions as received from employers and plan participants
- Distribution processing team – responsible for the processing of distributions, including making adjudication decisions for certain plan types

- Plan administration team – responsible for overall plan administration, trading, and reconciliation of assets with financial partners; also responsible for issuing periodic plan statements
- Customer service – provide customer service including the maintenance of toll-free telephone lines for calls from program participants

### Data Management

- The Relius application has a reporting module that enables MidAmerica personnel to query data from the application's Oracle database. Participant statements are generated and mailed on a quarterly or annual basis, depending on the type of plan. Periodic reports are also provided to the plan sponsors that show plan-level information (i.e. total contributions, distributions, balances, etc.)
- The Relevant Remitter application is also capable of generating reports. These reports are used by MidAmerica to provide its 415 and 402g limits compliance monitoring service for 403(b) TPA clients. In addition, Relevant Remitter is configured with alerts that will let MidAmerica personnel know if a participant is projected to exceed the 415 or 402g limits, in which case MidAmerica will contact the participant to make them aware of the issue.
- Custom reporting can also be utilized in Relevant Remitter. Additionally, Relevant Remitter can show plan and participant level information such as transaction counts, salary reduction reporting, and common remitting data.
- MidAmerica's system allows web-based participant inquiry for account balances, participant statements, distribution forms and other pertinent participant information. For plan sponsor reporting, the system allows for plan level inquiries as well as the capability to provide the plan sponsor with participant level reporting. Finally, the web-based system provides plan sponsor and vendor file upload and download functionality.

### CDN's Network Administration and Support Services

CDN was founded in 1992 as an outsourced provider of IT solutions. CDN performs the following services for MidAmerica:

*IT Direction and Supervision:* Assess the capabilities of the existing staff and recommend training opportunities. Conduct periodic evaluations and give appropriate feedback to the management team. If needed, write job descriptions for any new positions and participate in the evaluation and interview process for any new hires. Recommend changes to job descriptions for existing staff.

*System Configuration and Maintenance:* Configure and maintain production hardware including, but not limited to, servers, firewalls, routers, a web-filtering devices. CDN ensures that devices are updated with applicable vendor patches.

*System Availability:* Maintain system integrity and facilitate rapid recovery in case of system failure by recommending the appropriate support and supervision staffing, and participating in recovery operations. Recommend alternative means to continue operations until system operation is restored to normal levels. Create and test disaster recovery plans for all contingencies ranging from single system failure to catastrophic event. Coordinate with the IT staff and implement virus protection on all levels and maintain updated definition files. Prepare end-to-end documentation of the existing network including diagrams, OS versions, revision levels, configuration settings, hardware-specific settings down to component level of mission critical gear. Recommend processes and procedures to keep documentation current. Evaluate and recommend improvements to system security. Evaluate current procedures and if necessary implement improvements.

*Backup Administration:* Automated backup systems are configured and monitored to ensure that data and systems are backed up timely. System administrators are notified of each backup status whether successful or failed events occur.

*Network Monitoring:* Monitoring is in place to help detect network and system level failures. In the event of an outage, notifications are configured and sent to a distribution group including both CDN and MidAmerica personnel in real time via e-mail. Once alerted, the CDN engineers take corrective action to restore services.

*Project Consulting:* Review and recommend new technologies applicable to the business of the MidAmerica. Assist in determining which solution best fits the existing infrastructure, is scalable and has the best return on investments. Participate in selecting the appropriate vendor based on proximity and proven experience. This includes all network and system related technology as well as telephone systems, and peripherals. Review existing contracts and agreements with outside vendors and recommend opportunities to obtain competitive bids annually to receive the best terms possible while maintaining quality.

## **Scope Definition**

The scope of the engagement was limited to MidAmerica's plan administration services performed in its Lakeland, Florida, facility, as well as the network administration and support services provided by CDN.

### *Subservice Organizations*

CDN Partners, Inc. is a subservice organization that provided network administration and support services to MidAmerica during the review period. The services provided by CDN were included in the scope of the engagement.

### *Significant Changes During the Review Period*

No significant changes to the plan administration services system occurred during the review period.

---

## **CONTROL ENVIRONMENT**

The control environment at MidAmerica is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by the board of directors and management.

### **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 by example. Specific control activities that MidAmerica has implemented in this area are described below.

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

- Recurring background checks for existing employees are performed every five years.
- Drug screening tests are performed for employees as a component of the hiring process.

### **Commitment to Competence**

MidAmerica's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge. Specific control activities that MidAmerica has implemented in this area are described below.

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Skills testing are utilized during the hiring process to qualify the skills of personnel for certain positions.
- A training program has been developed to maintain the skill level of personnel in certain positions.

### **Board of Directors Participation**

MidAmerica's control consciousness is influenced significantly by its board of directors. The board of directors oversees management activities and meets on a regular basis to discuss matters pertinent to the organization's operations and to review financial results.

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

MidAmerica's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions and personnel. Specific control activities that MidAmerica has implemented in this area are described below.

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Management meetings are held on a weekly basis to discuss operational issues.
- 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 that 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 that 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, responsibility. These charts are communicated to employees and updated as needed.



## Human Resource Policies and Practices

MidAmerica's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities. Specific control activities that MidAmerica has implemented in this area are described below.

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

---

## RISK ASSESSMENT

MidAmerica has placed into operation a risk assessment process to identify and manage risks that could affect the organization's ability to provide reliable plan administration services for user organizations. This process requires management to identify significant risks in their areas of responsibility and to implement appropriate measures to address those risks. The risk assessment process occurs in real-time and during management's day to day activities. Management's active hands-on involvement allows anomalies in trends to be identified, analyzed, and mitigated immediately.

### Risk Identification

Management's recognition of risks that could affect the organization's ability to provide reliable plan administration services for its user organizations is generally implicit, rather than explicit. Management's involvement in the daily operations allows them to learn about risks through direct personal involvement with employees and outside parties, thus reducing the need for formalized and structured risk assessment processes. In addition, MidAmerica consults with outside legal counsel on a regular basis to ensure that the programs comply with applicable laws and regulations and utilize proper administrative and customer service procedures.

### Risks Analysis

Risk analysis is an essential process to MidAmerica's success. Management has implemented a process whereby the likelihood and impact of various risks to the in-scope services have been assessed. Once the significance and likelihood of risk have been assessed, management considers how the risk should be managed. This involves judgment based on assumptions about the risk, and reasonable analysis of costs associated with reducing the level of risk. Necessary actions are taken to reduce the significance or likelihood of the risk occurring, and identification of the control activities necessary to mitigate the risk. Management has identified

these control activities and documented them in the Control Objectives and Related Control Activities section below.

---

## CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES

### Integration with Risk Assessment

Along with assessing risks, management 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

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 below and also in Section 4 (the "Testing Matrices") of this report.

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

#### *Physical Security*

**Control Objective:** Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage and interference.

The MidAmerica office suite is located within a multi-tenant office building. The office suite doors are locked at all times. The front entrance is monitored by a receptionist during normal business hours. A badge access system is also in place to control access to the office suite 24 hours per day. Employees are assigned access levels within the badge access system and only certain employees have 24 hour access to the office suite. Administrative access to the badge system is only provided to the vice president of operations and the IT supervisor. Badge access permissions are reviewed on a quarterly basis by the vice president of operations. Visitors to the facility are required to sign a visitor log upon entry to the office suite and wear a visitors badge while onsite.

The server room is located within the office suite and secured via a cipher lock. Knowledge of the cipher lock code is restricted to management and CDN personnel.

#### *Environmental Security*

**Control Objective:** Control activities provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats.

The server room includes fire detection and suppression equipment that include a fire alarm system, water sprinklers, and a handheld fire extinguisher. The fire extinguisher was recently purchased and will be inspected by a third party on a periodic basis. The server room contains a dedicated air conditioning unit to maintain air temperature and humidity levels. An environmental monitoring application is configured to perform self-tests of the UPS system on a semi-monthly basis. The application is configured to send e-mail alerts to IT personnel when predefined temperature thresholds are exceeded. Production equipment is also connected to an

uninterruptible power supply (UPS) system to provide temporary power in the event of a power failure. Production IT equipment in the server room is placed in racks which elevate the equipment off of the floor to protect from localized flooding.

### *Computer Operations*

Control Objective: Control activities provide reasonable assurance that application and data files for the Plan Administration Services are backed up in a timely manner and securely stored.

Automated backup systems are configured and monitored to ensure that data and systems are backed up timely. System administrators are notified of each backup status whether successful or failed events occur.

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

Maintain system integrity and facilitate rapid recovery in case of system failure by recommending the appropriate support and supervision staffing, and participating in recovery operations. Recommend alternative means to continue operations until system operation is restored to normal levels. Create and test disaster recovery plans for all contingencies ranging from single system failure to catastrophic event. Coordinate with the IT staff and implement virus protection on all levels and maintain updated definition files. Prepare end-to-end documentation of the existing network including diagrams, OS versions, revision levels, configuration settings, hardware-specific settings down to component level of mission critical gear. Recommend processes and procedures to keep documentation current. Evaluate and recommend improvements to system security. Evaluate current procedures and if necessary implement improvements.

Monitoring is in place to help detect network and system level failures. In the event of an outage, notifications are configured and sent to a distribution group including both CDN and MidAmerica personnel in real time via e-mail. Once alerted, the CDN engineers take corrective action to restore services.

### *Information Security*

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

Active Directory controls access to the network domain and forces users to enter a unique account and valid password. Password parameters are enforced on user accounts, such as password expiration, minimum length, password history, password complexity and account lockout controls. The Windows web and database server authentication is derived from the network domain. Administrative access to the network domain and the operating systems are restricted to authorized personnel that include management and CDN personnel.

The Relius administration system, commercially licensed software, utilizes both a SQL Server database and an Oracle database. The common remitting and 403(b) TPA compliance monitoring application, Relevant Remitter, is a custom developed browser-based application that utilizes a SQL Server database. Administrative access to the databases is restricted to authorized personnel that include management and CDN personnel.

The Relius administration application and the Common Remitting application both require a valid user account name and password. The Relius administration application enforces certain password parameters that include minimum length, password expiration, password complexity and account lockout controls.

### *Data Communications*

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

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

### *Data Entry*

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

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

### *Contribution Processing*

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

A Participant Welcome Kit is sent to new participants once MidAmerica receives a contribution for the participant. The funds are initially invested based on the plan's default investment. The individual participant account is set up in the application for each fund and entity combination for which the participant is enrolled. The participant may elect to fill out an investment change form, included in the Welcome Kit (only applies to variable plans), to diversify their funds. An individual may have more than one account set up in the application, with each account containing one fund and entity combination.

Participant or employer funds are received via check or automated clearing house (ACH) with supporting allocation instructions for the contributions team. If the allocation instructions aren't submitted with the funds, the contributions team would contact the client to obtain the allocation instructions. The most recent monthly contribution deposit date per participant is recorded into the Relius application along with the participant name and address. Once the funds have been properly posted to the participant or employer accounts in the Relius application, a trading file is generated by the plan administration team that will instruct MidAmerica's financial partner of which assets to purchase. Prior to the trading file being sent to the financial partner, accounting personnel verifies that there are sufficient funds in the trust account for the purchasing of assets.

Salary Reduction Agreements (SRA) are submitted by the participants instructing MidAmerica as to how the participant wants their plan contributions allocated to the various vendors. MidAmerica records the SRA instructions in the Relevant Remitter application and then works with the employer's payroll department to ensure the employer is sending the participant's contributions to the correct vendor (must be on the employer's plan approved vendor list). Employers that elect to use MidAmerica's common remitting service send a lump sum and allocation instructions to MidAmerica, who then disburses the funds to the various approved vendors based on the participants' SRA allocation instructions. 402(g) and 415 compliance limits are monitored throughout the year and at year-end for clients who submit payroll data or are using common remitting services. Common remitting transactions are recorded in the Relevant Remitter application.

### *Customer Service*

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

MidAmerica ensures plan level compliance with applicable laws and plan limits. Participants are provided with customer service toll-free telephone numbers for plan assistance.

### *Distribution Processing*

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

*Single-sum:* MidAmerica receives a completed distribution request form from a plan participant. The mail receiving clerk date stamps distribution request forms received from the client. The forms are then forwarded to distribution processors. The distributions team updates participant records with information reported on the distribution form into the administration system. The distribution amount is calculated based on the most recently completed valuation. The distribution is then recorded in the Relius administration application, after which, the distribution will be paid. If applicable, copies of the distribution forms will be sent to the investment provider.

*FSA and HRA plans:* A distribution request and supporting documentation (i.e. explanation of benefits, receipts, invoices, etc.) is received by MidAmerica's distribution processing team. The distribution team reviews the distribution request, supporting documentation, and the employer's governing plan document to determine whether the documentation meets certain requirements (person that received the services, date of service, name of service provider, and amount). The distribution processing team then makes an adjudication decision as to whether the requested distribution qualifies under the employer's plan. The distribution team also verifies that the participant's account balance is sufficient to cover the funds requested. An export is run from the Relius application to generate a check printing file for distribution requests that were approved. Accounting personnel then perform a series of reconciliations during the check printing process.

*Employee Benefit Trust plans:* A distribution request is received by MidAmerica's distribution processing team requesting that either MidAmerica send the employer money from its Trust account or makes an allocation to one of the employer's plans. If the latter, there would have to be allocation instructions sent, just like the normal contribution process. With the Trust account plans, MidAmerica does not make an adjudication decision.

*3121 and APPLE plans:* At the end of the distribution period (quarterly for APPLE and monthly for 3121), the distribution processing team generates an authorization list for each client that shows all distribution requests for their plan participants. The client then makes an authorization decision for each distribution request and sends a file back to MidAmerica indicating whether each participant's request is authorized. MidAmerica then removes all denied request from each plan's distribution list. The approved distributions are then posted in the Relius application. An export is run from the Relius application to generate a check printing file for distribution requests that were approved. Accounting personnel then perform a series of reconciliations during the check printing process.

*Special Pay and Employer Sponsored 403(b) plans:* These are retirement plans for employees that can be one-time distribution requests or recurring requests. Additionally, there can be TPAs that manage these accounts on behalf of the employer. MidAmerica is the TPA for some accounts, but for others, there are separate TPAs that must approve the distribution prior to it being processed. The TPAs monitor compliance with certain plan regulations on behalf of the employers and ensure that distribution requests are in line with the eligibility rules as defined in the plan document. Once approved by either the employer or TPA, the approved distributions are posted in the Relius application. An export is run from the Relius application to generate a check printing file for distribution requests that were approved. Accounting personnel then perform a series of reconciliations during the check printing process.

Distribution drafts or checks are printed, signed, and mailed on a regular basis for all plan types listed above (based on a distribution schedule) from accounts established solely for the purpose of making benefit payments to plan participants. Drafts or checks are mailed directly to the participant's address on record unless the participant's benefit is payable to a third party. Accounting personnel reconcile balances in the disbursement accounts on a regular basis.

### *Valuation*

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

On a daily or monthly basis, any earnings reported by the trust are posted to the participant accounts. Earnings are calculated using date weighting. For ING valuations, 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. The team lead reviews the administration checklist and supporting documentation, and signs the administration checklist as evidence of their review. Reports are produced monthly that include a gains basis and participants that have zero or less balance.

For AUL valuations, a plan administrator reconciles the client's plan on the distribution partner's website to the administration system balance on a daily basis.

### *Participant Statements*

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

Update or change participant account data as requested in writing by the plan sponsor. Plan participants can also update personal information through the participant website. Statements are printed at the end of each plan year. After the statements have printed, plan administrators compare administration system reports to ensure that statements include the correct balance information. 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 printed. Statements are sent according to a predefined schedule.

### *HRA Claims Processing*

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

Claim adjudicators reviews the claims received for the required information, such as name, social security number, claim information and signature. If information was missing, the adjudicators would call the participant and obtain the information. Claims are denied for reason that include, but are not limited to, missing information, and the participant can't be contacted, or if the claimant is ineligible. Denial letters are sent out for any denied claims that notes the reason for the denial. If the claim is approved, the claim form is processed by a distribution processor who keys in the payee information and amount in the administration system and stamps the form as entered when complete.

### *403(b) TPA & Common Remitting Services*

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

A plan document and a plan adoption agreement are prepared for the client as a component of the plan setup process. The agreement includes an approved vendor list. Approved vendors are required to sign an information sharing agreement ("ISA"). Adjudicators review participant transaction requests to ascertain whether the request is allowed by the plan. Adjudicators stamp the request cover sheet to indicate approval if the request is allowed by the plan. If the request is denied, a denial letter is sent.

A common remitting service is offered to clients that elect the service. Those clients are required to sign a common remitting service agreement. The common remitting application reconciles payroll information received from the client to the expected amount in the common remitting application. The Relevant Remitter application then generates a list of errors for payroll amounts that did not match the expected amounts. The variances or issues are required to be resolved by 403(b) personnel before the payroll can be processed. The 403(b) plan administration manager or team supervisor finalizes payroll files after a review of a sample of files has been performed. The 403(b) plan administration manager or team supervisor reconciles finalized payroll files to the funds received by accounting on a daily basis. Evidence of the reconciliation is recorded on a common remitting checklist. 402(g) and 415 compliance limits are monitored throughout the year for clients who submit payroll data for common remitting. MidAmerica performed 402(g) and 415 compliance testing for their 403(b) clients on an annual basis if the clients provided the necessary data.

SRAs are assigned to vendors based on the information on the SRA form. The common remitting application is configured with a pre-populated listing of approved vendors. 403(b) plan administration personnel review any SRA configuration changes before the change is implemented.



---

## MONITORING

### Monitoring Activities

Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities, separate evaluation, or a combination of the two. Monitoring activities also include using information from communications with external parties such as user entities and regulatory comments that may indicate problems or highlight areas in need of improvement.

#### Ongoing Monitoring

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

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

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

#### Separate Evaluations

An independent financial audit and compliance audit take place to allow for monitoring of operations by third parties.

#### Internal and External Auditing

MidAmerica supports many user entities in their efforts to meet the regulatory demands of their industry or governing agency. MidAmerica has assisted user entities in successfully meeting the requirements of many compliance assessment and regulatory demands, including:

- SOC 1 / SSAE 16 examinations
- HIPAA
- IRS tax regulations
- Department of Labor
- US Department of Health & Human Services

### Reporting Deficiencies

The nature, timing and extent of the self-assessment tests and results are documented and reviewed by management. Deviations or deficiencies associated with controls are immediately escalated to management for immediate correction action. Corrective action, if required, is assigned to an individual and documented once those required actions are complete. Management reviews the deviations and corrective actions during periodic meetings.

---

## INFORMATION AND COMMUNICATION SYSTEMS

### Information Systems

The production information systems are located at the MidAmerica offices in Lakeland. A combination of custom developed, externally supported, and wholly purchased applications support the plan administration system.

The following provides a summary of systems used to provide the plan administration services:

- The core plan administration application, Relius Administration, is a commercially licensed software application that runs on Microsoft Windows workstations. The system utilizes both a SQL Server database and an Oracle database, which are housed on two separate Microsoft Windows servers. The application is used to process and record participant-level and plan-level transactions, and to generate client reports.
- Separate data entry applications have been developed using Microsoft Access and Microsoft Visual Studio. These applications utilize specific Microsoft SQL Server databases to store the input data that will be imported into Relius. Additionally, Optical Character Recognition (OCR) software is used to convert data from scanned document format to Microsoft Excel format files. The converted files are then imported into the Relius Administration application, which assimilates the input data using Data Entry Routines (DERs).
- The common remitting and 403(b) TPA compliance monitoring application, Relevant Remitter, is a custom developed browser-based application that runs on Microsoft Windows servers. The application utilizes a SQL Server database. The application is used to process and record 403(b) and common remitting transactions, and to generate client reports.

### Communication Systems

Upper management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities pertaining to internal controls. This includes the extent to which personnel understand how their activities relate to the work of others and the means of reporting exceptions to a higher level within MidAmerica. Management believes that open communication channels help ensure that exceptions are reported and acted on. For that reason, formal communication tools such as organizational charts, employee handbooks, training classes and job descriptions are in place. Management's communication activities are made electronically, verbally, and through the actions of management.

---

## COMPLEMENTARY CONTROLS AT USER ENTITIES

MidAmerica's plan administration services system is 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 plan administration services system to be solely achieved by MidAmerica's control activities. Accordingly, user entities, in conjunction with the plan administration services system, 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 specified control objectives described within this report are met:

### *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.

*Data Entry*

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

*Contribution Processing*

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

*Distribution Processing*

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

*403(b), TPA, & Common Remitting Services*

8. User entities are responsible for submitting the data needed to perform 402(g) and 415 compliance testing.

# SECTION 4

## TESTING MATRICES

## PHYSICAL SECURITY

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

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.01	A physical security policy is in place to guide personnel in determining access rights.	Inspected the physical security policy to determine that a physical security policy was documented.	No exceptions noted.
1.02	A receptionist monitors and controls access to the office suite during normal business hours.	Observed the suite entrance to determine that a receptionist monitored and controlled access to the office suite during normal business hours.	No exceptions noted.
1.03	Visitors are required to sign a visitors' log upon entering the office suite.	Observed the visitor access process to determine that visitors were required to sign a visitors log upon entering the office suite.	No exceptions noted.
		Inspected visitor logs for a nonstatistical sample of months during the review period to determine that a sign-in log was utilized to document visitor's access to the suite for each month sampled.	No exceptions noted.
1.04	Exterior doors to the office suite are locked at all times.	Inquired of the director of operations regarding office suite security to determine that exterior doors to the office suite were locked at all times.	No exceptions noted.
		Observed the office suite entrances to determine that exterior doors to the office suite were locked during business hours.	No exceptions noted.
1.05	A badge access system is in place to restrict access to the office suite.	Observed the exterior office entrances to determine that a badge access system was in place to restrict access to the office suite.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.06	Administrative access within the badge access system is restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• Vice president of operations</li> <li>• IT supervisor</li> </ul>	Inspected the badge access system administrator listing to determine that administrative access within the badge access system was restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• Vice president of operations</li> <li>• IT supervisor</li> </ul>	No exceptions noted.
1.07	Badge access is revoked as a component of the termination process.	Inquired of the IT supervisor regarding the access revocation process to determine that badge access was revoked as a component of the termination process.	No exceptions noted.
		Inspected the termination checklist and badge access listing for a nonstatistical sample of employees terminated during the review period to determine that badge access was revoked for each employee sampled.	No exceptions noted.
1.08	The vice president of operations reviews badge access permissions on a quarterly basis to help ensure that badge access permissions are authorized for each employee.	Inquired of the vice president of operations regarding the badge access review process to determine that the vice president of operations 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 nonstatistical sample of quarters during the review period to determine that the vice president of operations performed a badge access review for each quarter sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.09	<p>The server room door is secured via a cipher code lock. Knowledge of the server room door cipher code is restricted to persons holding the following positions:</p> <ul style="list-style-type: none"> <li>• VP of operations</li> <li>• Director of operations</li> <li>• Director of finance and administration</li> <li>• Director of customer service</li> <li>• TPA services manager</li> <li>• IT supervisor</li> <li>• Systems analyst</li> <li>• CDN IT administrators (3)</li> </ul>	Observed the server room entrance to determine that the server room door was secured via a cipher code lock.	No exceptions noted.
		<p>Inspected a listing of personnel with knowledge of the server room cipher lock code with the assistance of the IT supervisor to determine that knowledge of the server room door cipher lock code was restricted to persons holding the following positions:</p> <ul style="list-style-type: none"> <li>• VP of operations</li> <li>• Director of operations</li> <li>• Director of finance and administration</li> <li>• Director of customer service</li> <li>• TPA services manager</li> <li>• IT supervisor</li> <li>• Systems analyst</li> <li>• CDN IT administrators(3)</li> </ul>	No exceptions noted.

## ENVIRONMENTAL SECURITY

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

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.01	<p>The server room is equipped with the following fire detection and suppression equipment:</p> <ul style="list-style-type: none"> <li>• Fire alarm system</li> <li>• Water sprinklers</li> <li>• Handheld fire extinguisher</li> </ul>	<p>Observed the server room to determine that the server room was equipped with the following fire detection and suppression equipment:</p> <ul style="list-style-type: none"> <li>• Fire alarm system</li> <li>• Water sprinklers</li> <li>• Handheld fire extinguisher</li> </ul>	No exceptions noted.
2.02	<p>A dedicated air conditioning unit is in place to maintain air temperature and humidity levels within the server room.</p>	<p>Inquired of the IT supervisor regarding server room air conditioning to determine that a dedicated air conditioning unit was in place to maintain air temperature and humidity levels within the server room.</p>	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Observed the server room to determine that a dedicated air conditioning unit was in place.	No exceptions noted.
2.03	Production IT equipment is connected to uninterruptible power supply (UPS) systems to provide backup power in the event of a primary power failure, and to mitigate the risk of power surges impacting production infrastructure.	Inquired of the IT supervisor regarding UPS systems to determine that production IT equipment was connected to UPS systems to provide backup power in the event of a primary power failure, and to mitigate the risk of power surges impacting production infrastructure.	No exceptions noted.
		Observed the production IT equipment to determine that the equipment was connected to UPS systems.	No exceptions noted.
2.04	An environmental monitoring application is configured to perform self-tests of the UPS system on a semi-monthly basis.	Inspected the environmental monitoring application configurations to determine that an environmental monitoring application was configured to perform self-tests of the UPS system on a semi-monthly basis.	No exceptions noted.
2.05	An environmental monitoring application is configured to send e-mail alerts to IT personnel when predefined temperature thresholds are exceeded.	Inspected the environmental monitoring application configurations to determine that an environmental monitoring application was configured to send e-mail alerts to IT personnel when predefined temperature thresholds were exceeded.	No exceptions noted.
2.06	Production IT equipment in the server room is placed in racks which elevate the equipment off of the floor to protect from localized flooding.	Observed the server room to determine that production IT equipment in the sever room was placed in racks which elevated the equipment off of the floor to protect from localized flooding.	No exceptions noted.

## COMPUTER OPERATIONS

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

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.01	Documented data backup and restoration policies and procedures are in place to guide personnel in the backup and restoration processes.	Inspected the data backup and restoration policies and procedures to determine that backup and restoration policies and procedures were documented.	No exceptions noted.
3.02	IT personnel utilize an automated backup system to perform full backups of production data on a daily basis, Monday through Friday.	Inspected the automated backup system configurations and example backup logs generated during the review period to determine that an automated backup system was configured to perform full backups of production data on a daily basis, Monday through Friday.	No exceptions noted.
3.03	The automated backup system is configured to send backup completion status e-mail notifications to the IT supervisor.	Inspected the automated backup system notification configurations and an example backup completion status e-mail generated during the review period to determine that the automated backup system was configured to send backup completion status e-mail notifications to the IT supervisor.	No exceptions noted.
3.04	The automated backup system is configured to replicate backup data to a third party data center.	Inspected the automated backup system data replication configurations to determine that the automated backup system was configured to replicate backup data to a third party data center.	No exceptions noted.

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

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.01	Documented incident response policies and procedures are in place to guide personnel in reporting and responding to major information technology incidents.	Inspected the incident response procedures to determine that incident response policies and procedures were documented and included procedures for reporting and responding to incidents.	No exceptions noted.
4.02	IT personnel log operational issues into a ticketing system and assign personnel to monitor the status of the issues.	Inquired of the IT supervisor regarding the ticketing system to determine that IT personnel logged operational issues into a ticketing system and assigned personnel to monitor the status of the issues.	No exceptions noted.
		Inspected a listing of operational issues logged in the ticketing system during the review period to determine that operational issues were logged into a ticketing system.	No exceptions noted.
4.03	An enterprise monitoring application is configured to send e-mail notifications of production outages to CDN IT administrators.	Inspected the enterprise monitoring application configurations and an example e-mail notification generated during the review period to determine that an enterprise monitoring application sent e-mail notifications of production outages to CDN IT administrators.	No exceptions noted.
4.04	Antivirus software is installed on Windows servers and workstations to protect against certain virus definitions recognized by the software.	Inspected the antivirus software configurations to determine that antivirus software was installed on Windows servers and workstations to protect against certain virus definitions recognized by the software.	No exceptions noted.
4.05	The antivirus software is configured to update virus definitions every four hours.	Inspected the antivirus software configurations to determine that the antivirus software was configured to update virus definitions every four hours.	No exceptions noted.



## 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 Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>Network Authentication and Access</b>			
5.01	Users are required to authenticate via a user account and password before being granted access to the network domain.	Inspected a listing of network user accounts and the network authentication configurations to determine that users were required to authenticate via a network user account and password before being granted access to the network domain.	No exceptions noted.
5.02	The network domain is configured to enforce the following password requirements: <ul style="list-style-type: none"> <li>• Minimum length</li> <li>• Expiration interval</li> <li>• Password history</li> <li>• Password complexity</li> <li>• Invalid login attempt lockout threshold</li> </ul>	Inspected the network password and account lockout configurations to determine that the network domain was configured to enforce the following password requirements: <ul style="list-style-type: none"> <li>• Minimum length</li> <li>• Expiration interval</li> <li>• Password history</li> <li>• Password complexity</li> <li>• Invalid login attempt lockout threshold</li> </ul>	No exceptions noted.
5.03	Administrative access within the network domain is restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• IT supervisor</li> <li>• Systems analyst</li> <li>• CDN IT administrator</li> </ul>	Inspected the network administrator listing to determine that administrative access within the network domain was restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• IT supervisor</li> <li>• Systems analyst</li> <li>• CDN IT administrator</li> </ul>	No exceptions noted.
5.04	Access to the network domain is revoked as a component of the termination process.	Inquired of the IT supervisor regarding access revocation to determine that access to the network domain was revoked as a component of the termination process.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the termination checklist and the domain user account listing for a nonstatistical sample of employees terminated during the review period to determine that access to the network domain was revoked for each employee sampled.	No exceptions noted.
<b>Web and Database Server Operating System Access</b>			
5.05	Administrative access within the web and database server operating systems is restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• Director of operations</li> <li>• IT supervisor</li> <li>• Systems analyst</li> <li>• CDN IT administrator</li> <li>• Third party contractor</li> </ul>	Inspected the server operating system administrator listing for a nonstatistical sample of production servers and noted that administrative access within the sampled web and database servers' operating systems was restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• Director of operations</li> <li>• IT supervisor</li> <li>• Systems analyst</li> <li>• CDN IT administrator</li> <li>• Third party contractor</li> </ul>	No exceptions noted.
<b>Oracle Database Authentication and Access</b>			
5.06	Users are required to authenticate via a user account and password before being granted access to the database.	Inspected a screen print of the database authentication prompt to determine that users were required to authenticate via a user account and password before being granted access to the database.	No exceptions noted.
5.07	Administrative access within the database is restricted to default user accounts accessible by the IT supervisor.	Inquired of the IT supervisor regarding database access to determine that administrative access within the database was restricted to default user accounts accessible by the IT supervisor.	No exceptions noted.
		Inspected the listing of database roles and privileges to determine that administrative access within the database was restricted to shared user accounts.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>SQL Database Access</b>			
5.08	Administrative access within the database is restricted to a shared user account accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• Director of operations</li> <li>• IT supervisor</li> <li>• Systems analyst</li> <li>• Third party contractor</li> </ul>	Inquired of the IT supervisor regarding database access to determine that administrative access within the database was restricted to a shared user account accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• Director of operations</li> <li>• IT supervisor</li> <li>• Systems analyst</li> <li>• Third party contractor</li> </ul>	No exceptions noted.
		Inspected the listing of user accounts with administrative access to the database to determine that administrative access within the database was restricted to a shared user account.	No exceptions noted.
<b>Relius Administration System Application Authentication</b>			
5.09	Application users are required to authenticate via a user account and password before being granted access to the administration system application.	Inspected the application authentication configurations to determine that users were required to authenticate via a user account and password before being granted access to the administration application.	No exceptions noted.
5.10	The administration system application is configured to enforce the following password requirements: <ul style="list-style-type: none"> <li>• Minimum length</li> <li>• Expiration interval</li> <li>• Complexity requirements</li> <li>• Invalid login attempt lockout threshold</li> </ul>	Inspected the application password configurations to determine that the administration system application was configured to enforce the following password requirements: <ul style="list-style-type: none"> <li>• Minimum length</li> <li>• Expiration interval</li> <li>• Complexity requirements</li> <li>• Invalid login attempt lockout threshold</li> </ul>	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>Relius Administration System Application Access</b>			
5.11	Administrative access within the administration application is restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• Director of operations</li> <li>• Tax, accounting, and compliance director</li> <li>• Customer service supervisor</li> <li>• IT supervisor</li> <li>• Administrative assistants (2)</li> </ul>	Inspected the listing of administration application user accounts to determine that administrative access within the administration application was restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• Director of operations</li> <li>• Tax, accounting, and compliance director</li> <li>• Customer service supervisor</li> <li>• IT supervisor</li> <li>• Administrative assistants (2)</li> </ul>	No exceptions noted.
5.12	User accounts are assigned to predefined access roles to restrict access to certain functions within the administration system application.	Inspected the user access listing and security profile definitions to determine that user accounts were assigned to predefined access roles to restrict access to certain functions within the administration system application.	No exceptions noted.
5.13	Access to the administration system application is revoked as a component of the termination process.	Inquired of the IT supervisor regarding access revocation to determine that access to the administration system application was revoked as a component of the termination process.	No exceptions noted.
		Inspected the termination checklist and administration system application user account listing for a nonstatistical sample of employees terminated during the review period to determine that access to the administration system application was revoked for each employee sampled.	No exceptions noted.
<b>Relevant Remitter Application Authentication</b>			
5.14	Application users are required to authenticate via a user account and password before being granted access to the Relevant Remitter application.	Inspected the application authentication configurations to determine that users were required to authenticate via a user account and password before being granted access to the Relevant Remitter application.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>Relevant Remitter Application Access</b>			
5.15	Administrative access within the Relevant Remitter application is restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• IT supervisor</li> <li>• Plan administration manager</li> <li>• Account managers (2)</li> <li>• Team supervisors (2)</li> <li>• Account analyst</li> <li>• Accounting assistant</li> </ul>	Inspected the listing of Relevant Remitter application administrator accounts to determine that administrative access within the Relevant Remitter application was restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• IT supervisor</li> <li>• Plan administration manager</li> <li>• Account managers (2)</li> <li>• Team supervisors (2)</li> <li>• Account analyst</li> <li>• Accounting assistant</li> </ul>	No exceptions noted.
5.16	User accounts are assigned to predefined access roles to restrict access to certain functions within the Relevant Remitter application.	Inspected the user access listing and security profile definitions to determine that user accounts were assigned to predefined access roles to restrict access to certain functions within the Relevant Remitter application.	No exceptions noted.
5.17	Access to the Relevant Remitter application is revoked as a component of the termination process.	Inquired of the IT supervisor regarding access revocation to determine that access to the Relevant Remitter application was revoked as a component of the termination process.	No exceptions noted.
		Inspected the termination checklist and Relevant Remitter application user account listing for a nonstatistical sample of employees terminated during the review period to determine that access to the Relevant Remitter application was revoked for each employee sampled.	No exceptions noted.

## DATA COMMUNICATIONS

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

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.01	A stateful inspection firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram and firewall ruleset to determine that a stateful inspection firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
6.02	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 firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall rule.	No exceptions noted.
6.03	Network address translation (NAT) is enabled on the firewall to translate internally routable Internet Protocol (IP) addresses.	Inspected the listing of server IP addresses and the firewall ruleset to determine that NAT was enabled on the firewall to translate internally routable IP addresses.	No exceptions noted.
6.04	Administrative access within the firewall system is restricted to a user account accessible by CDN.	Inquired of the IT supervisor regarding firewall access to determine that administrative access within the firewall system was restricted to a user account accessible by CDN.	No exceptions noted.
		Inspected the firewall administrator listing to determine that administrative access within the firewall system was restricted to a single user account.	No exceptions noted.
6.05	Inbound Internet traffic terminates at a host in the demilitarized zone (DMZ) which is separate from the production network.	Inspected the network diagram to determine that inbound Internet traffic terminates at a host in the DMZ which was separate from the production network.	No exceptions noted.
6.06	Remote access to production environments is secured via encrypted virtual private network (VPN) connections.	Inspected the VPN encryption configurations to determine that remote access to production environments was secured via encrypted VPN connections.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.07	The ability to remotely connect to production servers via a VPN connection is restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• President</li> <li>• Vice president of operations</li> <li>• Director of operations</li> <li>• Director of IT</li> <li>• CDN</li> </ul>	Inspected the VPN configurations to determine that the ability to remotely connect to production servers via VPN connections was restricted to user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• President</li> <li>• Vice president of operations</li> <li>• Director of operations</li> <li>• Director of IT</li> <li>• CDN</li> </ul>	No exceptions noted.
6.08	An intrusion protection 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.

## 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 Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.01	The mail receiving clerk maintains a mail receiving log and enters the date contribution monies are received into a tracking spreadsheet.	Observed the mail receiving process to determine that the mail receiving clerk maintained a mail receiving log and entered the date contribution monies were received into a tracking spreadsheet.	No exceptions noted.
		Inspected tracking spreadsheets for a nonstatistical sample of months during the review period to determine that contribution monies were logged into a tracking spreadsheet for each month sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.02	Contribution reports and monies are sent to the accounting department and recorded in a check log.	Inquired of the director of operations regarding contributions to determine that contribution reports and monies were sent to the accounting department and recorded in a check log.	No exceptions noted.
		Inspected check logs for a nonstatistical sample of months during the review period to determine that contribution monies were recorded in a check log for each month sampled.	No exceptions noted.
7.03	The contribution monies recorded in the mail receiving clerk's tracking log and the accounting department's check log are reviewed by the accounting assistant on a monthly basis to ensure the amounts match.	Inquired of the director of operations regarding the monthly reconciliation process to determine that the contribution monies recorded in the mail receiving clerk's tracking log and the accounting department's check log were reviewed by the accounting assistant on a monthly basis to ensure the amounts matched.	No exceptions noted.
		Inspected the contribution money reconciliations for a nonstatistical sample of months during the review period to determine that the logs were reconciled for each month sampled.	No exceptions noted.

## 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 Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
8.01	Documented contribution processing procedures are in place to guide personnel in the contributions processes.	Inspected the contribution processing procedures to determine that documented contribution procedures were in place.	No exceptions noted.



#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
8.02	Contribution information is scanned into a document imaging application for archiving and retrieval of information.	Inquired of the director of operations regarding document imaging to determine that contribution information was scanned into a document imaging application for archiving and retrieval of information.	No exceptions noted.
		Inspected the imaging application configurations and example imaged contribution documentation to determine that contribution documentation was scanned into a document imaging application.	No exceptions noted.
8.03	Contribution information received from clients electronically is balanced in total to the check, wire, or ACH amount received.	Inquired of the director of operations 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.
8.04	Enrollment information is entered into the administration system application from standard enrollment forms.	Observed the enrollment entry process to determine that enrollment information was entered into the administration system application from standard enrollment forms.	No exceptions noted.
8.05	Participant contribution information is imported into the administration system application. The contribution processing supervisor reviews the imported data in the administration application and documents evidence of review in a spreadsheet.	Inquired of the director of operations regarding contribution information review to determine that participant contribution information was imported into the administration system application, and the information was reviewed by the contribution processing supervisor.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the peering spreadsheet for a nonstatistical sample of months during the review period to determine that the contribution processing supervisor reviewed imported data in the administration system and documented evidence of review on the peering spreadsheet for each month sampled.	No exceptions noted.

## 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 Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
9.01	Management meets to discuss customer service issues on a weekly basis.	Inspected the management meeting minutes for a nonstatistical sample of weeks during the review period to determine that management met to discuss customer service issues during each week sampled.	No exceptions noted.
9.02	Customer service personnel undergo training to obtain knowledge of the various plan attributes.	Inquired of the director of operations regarding training to determine that customer service personnel underwent training to obtain knowledge of the various plan attributes.	No exceptions noted.
		Inspected evidence of customer service personnel training courses completed during the review period to determine that customer service personnel underwent training of the various plan attributes.	No exceptions noted.
9.03	Customer service personnel utilize automated call software to provide statistical analysis regarding customer service phone activity.	Inquired of the director of operations 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.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected example 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.
9.04	Customer service management personnel silently monitor customer service calls for quality assurance purposes on a periodic basis. Call performance is formally assessed for each customer service representative on a semi-annual basis.	Inquired of the director of operations regarding call monitoring to determine that customer service management personnel silently monitored customer service calls for quality assurance purposes on a periodic basis.	No exceptions noted.
		Inspected the most recent employee evaluations for a nonstatistical sample of customer service representatives to determine that call performance was formally assessed during the review period for each customer service representative sampled.	No exceptions noted.
9.05	Customer satisfaction surveys are randomly sent to clients throughout the year to monitor the performance of customer service personnel.	Inquired of the director of operations regarding customer satisfaction surveys to determine that customer satisfaction surveys were randomly sent to clients throughout the year to monitor the performance of customer service personnel.	No exceptions noted.
		Inspected example customer satisfaction surveys received during the review period to determine that customer satisfaction surveys were sent to clients to monitor the performance of customer service personnel.	No exceptions noted.

## DISTRIBUTION PROCESSING

**Control Objective Specified** Control activities provide reasonable assurance that distribution requests are entered and processed accurately and timely.  
**by the Service Organization:**

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
10.01	Documented distribution procedures and schedules are in place to guide personnel in the distribution processes and date requirements.	Inspected the distribution procedures and schedules to determine that documented distribution procedures and schedules were in place.	No exceptions noted.
10.02	Recurring Special Pay / HRA distributions are entered into a tracking spreadsheet to help ensure that the recurring payments are entered in the correct time period.	Inquired of the director of operations regarding recurring payouts to determine that recurring Special Pay / HRA distributions were entered into a tracking spreadsheet to help ensure that the recurring payments were entered in the correct time period.	No exceptions noted.
		Inspected the recurring distribution spreadsheet to determine that recurring Special Pay / HRA distributions were entered into a tracking spreadsheet.	No exceptions noted.
10.03	A checklist is created for each plan distribution run to guide administration and accounting personnel during the distribution process.	Inquired of the director of operations regarding the distribution process to determine that a checklist was created for each plan distribution run to guide administration and accounting □□□□□□□□□□□□□□□□□□□□ □□□□□□□□□□□□□□□□□□□□	No exceptions noted.
		Inspected the distribution checklist for a nonstatistical sample of distributions processed during the review period to determine that a checklist was created for each distribution sampled.	No exceptions noted.
10.04	The mail receiving clerk date stamps distribution request forms received from the client. The forms are then forwarded to distribution processors.	Inquired of the director of operations regarding mail receiving to determine that after the distribution requests were date stamped, they were forwarded to the distribution processors.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the distribution request forms for a nonstatistical sample of distributions processed during the review period to determine that the mail receiving clerk date stamped each distribution request form sampled.	No exceptions noted.
10.05	Distribution processors enter distribution request forms into the administration system application. The new requests are placed in a suppressed status.	Observed the data entry process to determine that distribution processors entered distribution request forms into the administration system application and the new requests were placed in a suppressed status.	No exceptions noted.
10.06	The administration supervisor compares the information entered into the administration system application to the distribution form to ensure that the information entered is correct and conforms to the distribution processing guidelines. The distribution checklist is initiated upon completion of this task.	Inquired of the director of operations regarding distributions to determine that the administration supervisor compared the information entered into the administration system application to the distribution form to ensure that the information entered was correct and conformed to the distribution processing guidelines.	No exceptions noted.
		Inspected the distribution checklist for a nonstatistical sample of distributions processed during the review period to determine that evidence of review was documented for each distribution sampled.	No exceptions noted.
10.07	Access to post the suppressed distribution requests in the administration system application is restricted to administration application user accounts accessible by persons holding the following positions: <ul style="list-style-type: none"> <li>• Plan administrator</li> <li>• Distribution processors (5)</li> </ul>	Inspected the administration system user access listing to determine that access to post the suppressed distribution requests in the administration system application was restricted to administration application user accounts accessible by persons holding the following positions <ul style="list-style-type: none"> <li>• Plan administrators</li> <li>• Distribution processors (5)</li> </ul>	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
10.08	For Section 3121 and APPLE distribution requests, an approved distribution authorization report must be obtained from the client before the distributions are posted in the administration application.	Inquired of the director of operations regarding the distribution authorization report to determine that for Section 3121 and APPLE distribution requests, an approved distribution authorization report must have been obtained from the client before the distributions were posted in the administration application.	No exceptions noted.
		Inspected the 3121 distribution authorization reports for a nonstatistical sample of clients and months during the review period to determine that a signed distribution authorization report was obtained for each client and month sampled.	No exceptions noted.
		Inspected the Apple distribution authorization reports for a nonstatistical sample of clients and quarters during the review period to determine that a signed distribution authorization report was obtained for each client and quarter sampled.	No exceptions noted.
10.09	The plan administrator resolves possible errors in payee amounts which are identified on an error report, before check processing can continue.	Inquired of the director of operations regarding error resolution to determine that possible errors were resolved by the plan administrator before check processing continued.	No exceptions noted.
		Inspected an example error report to determine that errors in payee amounts were identified on an error report.	No exceptions noted.
10.10	The distribution processor verifies the number of distribution payments exported from the proprietary utility tool to the checklist created by administration personnel. The distribution checklist is initialed upon completion of this task.	Inquired of the director of operations regarding the distribution payment count process to determine that the distribution processor verified the number of distribution payments exported from the proprietary utility tool to the checklist created by administration personnel.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the distribution checklist for a nonstatistical sample of distributions processed during the review period to determine that the checklist was initialed to evidence that the distribution payment file count was verified for each distribution sampled.	No exceptions noted.
10.11	Accounting personnel review the detail of the check file loaded into the commercial check writing application to ensure that the format of the checks is correct and that the number of checks printed matches the number of checks listed on the distribution run checklist. The distribution checklist is initialed upon completion of this task.	Inquired of the director of operations regarding the check file review process to determine that accounting personnel reviewed the detail of the check file loaded into the commercial check writing application to ensure that the format of the checks was correct and that the number of checks printed matched the number of checks listed on the distribution run checklist.	No exceptions noted.
		Inspected the distribution checklist for a nonstatistical sample of distributions processed during the review period to determine that the checklist was initialed to evidence that the printed checks were reviewed and counted for each distribution sampled.	No exceptions noted.
10.12	A password is required to print checks in the check printing application.	Inspected a screen print of the check printing application authentication prompt to determine that a password was required to print checks in the check printing application.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
10.13	<p>Access to print checks in the check printing application is restricted to user accounts accessible by persons holding the following positions:</p> <ul style="list-style-type: none"> <li>• VP of operations</li> <li>• Tax, accounting, and compliance director</li> <li>• Accounting supervisor</li> <li>• Senior accounting assistant</li> </ul>	<p>Inspected a listing of the check printing application users with the assistance of the vice president of operations to determine that access to print checks in the check printing application was restricted to user accounts accessible by persons holding the following positions:</p> <ul style="list-style-type: none"> <li>• VP of operations</li> <li>• Tax, accounting, and compliance director</li> <li>• Accounting supervisor</li> <li>• Senior accounting assistant</li> </ul>	No exceptions noted.
10.14	A check log is maintained which details the last check number used and the number of checks printed.	Inspected the check log for the review period to determine that a check log was maintained during the review period which detailed the last check number used and the number of checks printed.	No exceptions noted.
10.15	The administration application is updated with the amount of the distribution, check number, and issue date. Completion of this task is recorded on the distribution checklist.	Inquired of the director of operations regarding the application update process to determine that the administration application was updated with the amount of the distribution, check number, and issue date.	No exceptions noted.
		Inspected the distribution checklist for a nonstatistical sample of distributions processed during the review period to determine that the checklist was initialed to evidence that the administration application was updated with the distribution amount, check number, and issue date for each distribution sampled.	No exceptions noted.



#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
10.16	The tax, accounting, and compliance director or accounting supervisor performs a final review of the printed checks to ensure that the total amount and the count of the printed checks match the amount that was previously approved. The distribution checklist is initialed upon completion of this task.	Inquired of the director of operations regarding the final check review process to determine that the tax, accounting, and compliance director or the accounting supervisor performed a final review of the printed checks to ensure that the total amount and the count of the printed checks matched the amount that was previously approved.	No exceptions noted.
		Inspected the distribution checklist for a nonstatistical sample of distributions processed during the review period to determine that the checklist was initialed to evidence that the final check review was performed for each distribution sampled.	No exceptions noted.
10.17	A positive pay file is created and sent to the financial institution. The accounting assistant reviews daily notices from the financial institution which identifies possible fraudulent checks for a decision on whether or not to pay the check. Only the vice president of operations and the tax, accounting, and compliance director have access to pay/return positive pay notifications.	Inquired of the tax, accounting, and compliance director regarding access to the banking website to determine that only the vice president of operations and the tax, accounting, and compliance director had the access to pay/return positive pay notifications.	No exceptions noted.
		Observed the positive pay review process to determine that a positive pay file was created and sent to the financial institution and that the staff accountant reviewed notices from the financial institution which identified possible fraudulent checks for a decision on whether or not to pay the check.	No exceptions noted.

## VALUATION

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that account valuation procedures are performed accurately.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>ING Valuation</b>			
11.01	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 nonstatistical sample of months during the review period to determine that a month end valuation checklist was utilized to guide plan administrators in completing valuation tasks for each month sampled.	No exceptions noted.
11.02	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 director of operations regarding the trust statement reconciliation process to determine that plan administrators reconciled the posted participant contributions and distributions to the trust statement to determine the earnings or dividends that should be posted to the administration system.	No exceptions noted.
		Inspected the month end valuation checklist for a nonstatistical sample of months during the review period to determine that the month end valuation checklist was initialed to evidence that contributions and distributions were reconciled to the trust statement for each month sampled.	No exceptions noted.
11.03	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 director of operations 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.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the month end valuation checklist for a nonstatistical sample of months during the review period to determine that the month end valuation checklist was initialed to evidence that a negative balance report was produced for each month sampled.	No exceptions noted.
11.04	A gains basis and participants that have zero or less balance reports are produced on a monthly basis and provided to the team leads for review.	Inquired of the director of operations regarding the gains basis reports to determine that a gains basis and participants that had zero or less balance reports were produced on a monthly basis and provided to the team leads for review.	No exceptions noted.
		Inspected the gains basis and participants that had zero or less gains reports for a nonstatistical sample of months during the review period to determine that a gains basis and participants that have zero or less gains reports were produced for each month sampled.	No exceptions noted.
11.05	The team lead 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 nonstatistical sample of months during the review period to determine that the team lead signed the administration checklist as evidence of their review for each month sampled.	No exceptions noted.
<b>AUL Valuation</b>			
11.06	A plan administrator reconciles the client's plan on the distribution partner's website to the administration system balance on a daily basis.	Inquired of the director of operations regarding the daily earnings reconciliation to determine that a plan administrator reconciles the client's plan on the distribution partner's website to the administration system balance on a daily basis.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected reconciliation reports for a nonstatistical sample of dates during the review period to determine that the client's plan on the distribution partner's website was reconciled to the administration system balance for each date sampled.	No exceptions noted.

## 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 Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
12.01	Documented statement printing procedures are in place to guide plan administrators in participant statement printing process.	Inspected the participant statement instructions to determine that documented statement printing procedures were in place.	No exceptions noted.
12.02	A statement schedule outlines when the statements are required to be printed and mailed for each plan.	Inspected the statement schedule to determine that a statement schedule outlined when the statements were required to be printed and mailed for each plan.	No exceptions noted.
12.03	Plan administrators compare administration system reports to ensure that statements include the correct balance information.	Inquired of the director of operations 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.
		Observed the participant statement review process to determine that plan administrators compared administration system reports to ensure that statements included the correct balance information.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
12.04	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 printed.	Inquired of the director of operations 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 printed.	No exceptions noted.
		Inspected example statement logs to determine that a log of the number of statements printed was created by the plan administrators and reviewed by the team leads.	No exceptions noted.
12.05	The plan administrators compare a summary page of the printed statements to the valuation report to ensure that the information from the valuation report matches the hard copy statement.	Inquired of the director of operations regarding the statement review process to determine that a summary page of the printed statements was compared to the valuation report by the plan administrators to ensure that the information from the valuation report matched the hard copy statement.	No exceptions noted.
		Inspected example statement reconciliation documentation to determine that a summary page of the printed statements was compared to the valuation report by the plan administrators.	No exceptions noted.

## 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 Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
13.01	Documented procedures are in place to guide distribution personnel in the claims payment and review process.	Inspected the distribution policies and procedures to determine that documented procedures were in place to guide distribution personnel in the claims payment and review process.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
13.02	Claims adjudicators are trained on the HRA claims adjudication and distribution process as a component of the hiring process.	Inquired of the director of operations 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 claims adjudication training documentation to determine that a formal training program was in place.	No exceptions noted.
13.03	The claims adjudicator reviews the claim to ensure the claim form is signed and the necessary information is included.	Inquired of the director of operations 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 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.
13.04	Reference materials are maintained to guide claims adjudicators in establishing the reimbursement eligibility of submitted claims.	Inspected the reference materials to determine that reference materials were maintained to guide claims adjudicators in establishing the reimbursement eligibility of submitted claims.	No exceptions noted.
13.05	If the claim is denied, the claims adjudicator notifies the participant of the denial.	Inquired of the director of operations regarding denied claims to determine that if the claim was denied, the claims adjudicator notified the participant of the denial.	No exceptions noted.
		Inspected an example denial letter to determine that a denial letter template was in place if the claim was denied.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
13.06	If the claim is approved, the claim form is processed by a distribution processor who keys in the payee information and amount in the administration system and stamps the form as entered when complete.	Inquired of the director of operations 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 the administration system and stamps the form as entered when complete.	No exceptions noted.
		Inspected the claim form for a nonstatistical sample of distributions processed during the review period to determine that the claim form was stamped as entered for each distribution sampled.	No exceptions noted.

## 403(b) TPA & COMMON REMITTING SERVICES

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

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
14.01	Documented policies and procedures are in place to guide personnel in the 403(b) administration process.	Inspected the policies and procedures to determine that 403(b) policies and procedures were documented.	No exceptions noted.
14.02	A plan document and a plan adoption agreement are prepared for the client as a component of the plan setup process.	Inquired of the plan administration manager regarding plan documents to determine that a plan document and a plan adoption agreement were prepared as a component of the client setup process.	No exceptions noted.
		Inspected the plan adoption agreement for a nonstatistical sample of clients enrolled during the review period to determine that a plan adoption agreement was prepared for each client sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
14.03	An approved vendor list is prepared for the client as a component of the plan setup process.	Inspected the approved vendor list for a nonstatistical sample of clients enrolled during the review period to determine that an approved vendor list was prepared for each client sampled.	No exceptions noted.
14.04	Approved vendors are required to sign an information sharing agreement ("ISA".)	Inspected the ISA's for a nonstatistical sample of clients enrolled during the review period to determine that the approved vendors signed an ISA for each client sampled.	No exceptions noted.
14.05	Adjudicators review participant transaction requests to ascertain whether the request is allowed by the plan. Adjudicators stamp the request cover sheet to indicate approval if the request is allowed by the plan.	Inquired of the plan administration manager regarding the adjudication process to determine that adjudicators reviewed participant transaction requests to ascertain whether the request was allowed by the plan.	No exceptions noted.
		Observed the transaction request review process to determine that adjudicators stamped the request cover sheet if the request was allowed by the plan.	No exceptions noted.
14.06	A denial letter is sent to participants if their transaction request is denied.	Inquired of the plan administration manager regarding denial letters to determine that a denial letter was sent to participants if their transaction request was denied.	No exceptions noted.
		Inspected an example denial letter to determine that a denial letter template was in place if the claim was denied.	No exceptions noted.
<b>Internal Common Remitting</b>			
14.07	A common remitting service is offered to clients that elect the service. Those clients are required to sign a common remitting service agreement.	Inquired of the plan administration manager regarding common remitting to determine that a common remitting service was offered to clients and that clients were required to sign a common remitting service agreement.	No exceptions noted.



#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the common remitting service agreement for a nonstatistical sample of common remitting clients enrolled during the review period to determine that a common remitting service agreement was signed by each client sampled.	No exceptions noted.
14.08	The common remitting application reconciles payroll information received from the client to the expected amount in the common remitting application. Any variances or issues must be resolved by 403(b) personnel before the payroll can be processed.	Inquired of the plan administration manager regarding the common remitting process to determine that the common remitting application reconciled payroll information received from the client to the expected amount in the common remitting application, and that any variances or issues must be resolved by 403(b) personnel before the payment can be processed.	No exceptions noted.
		Observed the common remitting process to determine that the common remitting application reconciled payroll information received from the client to the expected amount in the common remitting application.	No exceptions noted.
14.09	The 403(b) plan administration manager or team supervisor finalizes payroll files in a “releasable” status, which archives contributions in plan and participant records in the common remitting application.	Observed the common remitting process to determine that the 403(b) plan administration manager or team supervisor finalized payroll files in a “releasable” status, which archived contributions in plan and participant records in the common remitting application.	No exceptions noted.
14.10	The 403(b) plan administration manager or team supervisor reconciles finalized payroll files to the funds received by accounting on a daily basis. Evidence of the reconciliation is recorded on a common remitting checklist.	Inspected the common remitting checklists for a nonstatistical sample of dates during the review period to determine that the 403(b) plan administration manager or team supervisor reconciled finalized payroll files to the funds received by accounting and recorded completion of the reconciliation on a common remitting checklist for each date sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>Salary Reduction Agreements (SRAs)</b>			
14.11	SRAs are assigned to vendors based on the information on the SRA form. The common remitting application is configured with a pre-populated listing of approved vendors.	Observed the SRA entry process to determine that SRAs were assigned to vendors based on the information on the SRA form.	No exceptions noted.
		Inspected the common remitting application configurations to determine that the common remitting application was configured with a pre-populated listing of approved vendors.	No exceptions noted.
14.12	SRA configuration changes in the common remitting application are placed in a pending status until they are reviewed and approved by 403(b) plan administration personnel.	Inquired of the plan administration manager regarding the SRA change process to determine that SRA configuration changes in the common remitting application were placed in a pending status until they were reviewed and approved by 403(b) plan administration personnel.	No exceptions noted.
		Observed the SRA entry process to determine that SRA configuration changes in the common remitting application were placed in a pending status until they were reviewed and approved by 403(b) plan administration personnel.	No exceptions noted.
<b>Compliance Testing</b>			
14.13	402(g) and 415 compliance limits are monitored throughout the year for clients who submit payroll data for common remitting.	Observed the compliance monitoring process to determine that 402(g) and 415 compliance limits were monitored throughout the year for clients who submitted payroll data for common remitting.	No exceptions noted.
14.14	402(g) and 415 compliance testing is performed on an annual basis.	Inquired of the plan administration manager regarding compliance testing to determine that 402(g) and 415 compliance testing was performed on an annual basis.	No exceptions noted.
		Inspected the most recent compliance testing results for an example client to determine that 402(g) and 415 compliance testing was performed during the review period.	No exceptions noted.

# SECTION 5

## OTHER INFORMATION PROVIDED BY MANAGEMENT

---

## DISASTER RECOVERY PLANNING

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

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