

# System and Organization Controls Report SOC 1<sup>®</sup> Type 2

Report on the Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls

Related to Benefit Plan Administrative Services, Inc.'s Plan Administration and Recordkeeping Service

Under the AICPA, Statement on Standards for Attestation Engagements No. 18 (SSAE No. 18), Section AT-C 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*

For the Period November 1, 2020 to October 31, 2021



# Table of Contents

<b>SECTION I: Independent Service Auditor’s Report</b> .....	<b>1</b>
<b>SECTION II: Assertion of Benefit Plan Administrative Services, Inc.’s Management</b> .....	<b>5</b>
<b>SECTION III: System Description Provided by Benefit Plan Administrative Services, Inc.</b> .....	<b>8</b>
<b>Company History &amp; Overview</b> .....	<b>9</b>
<b>Scope of Report</b> .....	<b>10</b>
Key Systems for the Plan Administration and Recordkeeping Service.....	11
Ancillary Tools and Systems .....	12
<b>Relevant Aspects of the Control Environment, Risk Assessment, Monitoring, Management Oversight, and Governance</b> .....	<b>14</b>
<b>Description of Controls</b> .....	<b>18</b>
Benefit Administration and Transaction Processing.....	19
Participant Plan Changes .....	20
Participant Deferrals and Contributions .....	21
Trade Processing .....	22
Participant Disbursements and Payments .....	23
Customer Statements.....	24
VEBA and Health & Welfare Plans Claims Processing.....	25
Defined Benefit and Other Postemployment Benefits Valuation.....	25
Defined Benefit Administration .....	26
Changes to pension plan participant data are processed throughout the year based on data provided by the plan sponsor. ....	26
Software Development and Maintenance .....	26
Logical Access.....	28
Backups.....	30
System Processing and Performance Monitoring .....	30
Physical Security .....	31
Subservice Organization Monitoring Controls .....	31
<b>Complementary User Entity Controls</b> .....	<b>33</b>
<b>Subservice Organizations</b> .....	<b>34</b>
<b>SECTION IV: Independent Service Auditor’s Description of Tests of Controls and Results</b> .....	<b>36</b>
Overview of Crowe LLP’s Test Procedures .....	37
Control Objective 1: Management Oversight and Governance .....	38
Control Objective 2: Benefit Administration and Transaction Processing.....	39
Control Objective 3: Participant Plan Changes .....	43
Control Objective 4: Participant Deferrals and Contributions.....	44
Control Objective 5: Trade Processing.....	46
Control Objective 6: Participant Disbursements and Payments .....	47
Control Objective 7: Customer Statements .....	48
Control Objective 8: VEBA, HRA, FSA, and HSA Claims Processing .....	49
Control Objective 9: Defined Benefit and Other Postemployment Benefits Administration .....	50
Control Objective 10: Software Development and Maintenance .....	52
Control Objective 11: Logical Access.....	53
Control Objective 12: Backups.....	55
Control Objective 13: System Processing and Performance Monitoring .....	56
Control Objective 14: Physical Security .....	57
Control Objective 15: Subservice Organization Monitoring.....	58
<b>SECTION V: Other Information Provided by Benefit Plan Administrative Services, Inc. (Unaudited)</b> .....	<b>59</b>

# SECTION I: Independent Service Auditor's Report

## INDEPENDENT SERVICE AUDITOR'S REPORT

To Benefit Plan Administrative Services, Inc., a wholly owned subsidiary of Community Bank System, Inc.

### Scope

We have examined Benefit Plan Administrative Services, Inc.'s (BPAS or service organization), a wholly owned subsidiary of Community Bank System, Inc., description of its Plan Administration and Recordkeeping Service entitled "System Description Provided by Benefit Plan Administrative Services, Inc." for providing bundled daily recordkeeping, administration, clearing, custodial and / or directed trustee services (from various BPAS entities or subsidiaries) throughout the period November 1, 2020 to October 31, 2021, (description) and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Assertion of Benefit Plan Administrative Services, Inc.'s Management" (assertion). The controls and control objectives included in the description are those that management of BPAS believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Plan Administration and Recordkeeping Service that are not likely to be relevant to user entities' internal control over financial reporting.

BPAS uses a subservice organization to provide the services described in Section III. The description includes only the control objectives and related controls of BPAS and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by BPAS can be achieved only if complementary subservice organization controls assumed in the design of BPAS's controls are suitably designed and operating effectively, along with the related controls at BPAS. Our examination did not extend to controls of the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of BPAS's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

The information included in Section V, "Other Information Provided by Benefit Plan Administrative Services, Inc. (Unaudited)" is presented by management of BPAS to provide additional information and is not a part of BPAS's description of its Plan Administration and Recordkeeping Service made available to user entities during the period November 1, 2020 to October 31, 2021. Information about BPAS's Disaster Recovery and Business Continuity Planning, Privacy Policies, and Regulations and Compliance have not been subjected to the procedures applied in the examination of the description of the Plan Administration and Recordkeeping Service and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the Plan Administration and Recordkeeping Service, and accordingly, we express no opinion on it.

### **Service Organization's Responsibilities**

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

### **Service Auditor's Responsibilities**

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

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period November 1, 2020 to October 31, 2021. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

### **Inherent Limitations**

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

### Description of Tests of Controls

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

### Opinion

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

- a. the description fairly presents BPAS's Plan Administration and Recordkeeping Service that was designed and implemented throughout the period November 1, 2020 to October 31, 2021.
- b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period November 1, 2020 to October 31, 2021, and the subservice organization and user entities applied the complementary controls assumed in the design of BPAS's controls throughout the period November 1, 2020 to October 31, 2021.
- c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period November 1, 2020 to October 31, 2021, if complementary subservice organization and user entity controls assumed in the design of BPAS's controls operated effectively throughout the period November 1, 2020 to October 31, 2021.

### Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of BPAS, user entities of BPAS's Plan Administration and Recordkeeping Service during some or all of the period November 1, 2020 to October 31, 2021, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than the specified parties.

  
Crowe LLP

South Bend, Indiana  
March 8, 2022

## SECTION II: Assertion of Benefit Plan Administrative Services, Inc.'s Management



March 8, 2022

### **Assertion of Benefit Plan Administrative Services, Inc.'s Management**

We have prepared the description of Benefit Plan Administrative Services, Inc.'s (BPAS or service organization), a wholly owned subsidiary of Community Bank System, Inc., Plan Administration and Recordkeeping Service entitled, "System Description Provided by Benefit Plan Administrative Services, Inc." for processing user entities' transactions throughout the period November 1, 2020 to October 31, 2021 (description), for user entities of the system during some or all of the period November 1, 2020 to October 31, 2021, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by the subservice organization and user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

BPAS uses a subservice organization to provide the services described in Section III. The description includes only the control objectives and related controls of BPAS and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by BPAS can be achieved only if complementary subservice organization controls assumed in the design of BPAS's controls are suitably designed and operating effectively, along with the related controls at BPAS. The description does not extend to controls of the subservice organization.

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

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

- a. the description fairly presents the Plan Administration and Recordkeeping Service made available to user entities of the system during some or all of the period November 1, 2020 to October 31, 2021 for processing user entities' transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description
  - i. presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable,
    - (1) the types of services provided, including, as appropriate, the classes of transactions processed.
    - (2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.
    - (3) the information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.



- (4) how the system captures and addresses significant events and conditions other than transactions.
    - (5) the process used to prepare reports and other information for user entities.
    - (6) services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.
    - (7) the specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls.
    - (8) other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.
  - ii. includes relevant details of changes to the service organization's system during the period covered by the description.
  - iii. does not omit or distort information relevant to the service organization's system, while acknowledging that the description is prepared 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 and Recordkeeping Service that each individual user entity of the system and its auditor may consider important in its own particular environment.
- b. the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period November 1, 2020 to October 31, 2021 to achieve those control objectives if the subservice organization and user entities applied the complementary controls assumed in the design of BPAS's controls throughout the period November 1, 2020 to October 31, 2021. 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 of the service organization.
  - ii. the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.
  - iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

**Benefit Plan Administrative Services, Inc**

SECTION III: System Description Provided by Benefit Plan  
Administrative Services, Inc.

## Company History & Overview

Benefit Plans Administrators was established in 1973 as an independent third-party administrator of qualified pension and profit-sharing plans. In 1996, the Company was acquired by Community Bank System, Inc. (CBSI) and was rebranded as Benefit Plans Administrative Services, Inc. (BPAS). BPAS and Community Bank, NA are the two primary operating subsidiaries of CBSI. BPAS includes several legal entities: BPAS, LLC; BPAS Actuarial & Pension Services, LLC (formerly Harbridge Consulting Group); Hand Benefits and Trust (HB&T); Hand Securities, Inc. (HSI) and BPAS Trust Company of Puerto Rico. BPAS provides a range of services to meet the needs of plan sponsors and financial intermediary partners, across 12 lines of business. This includes Plan Administration & Recordkeeping Services; IRA Services; TPA Services; Actuarial and Pension Services; MyPlanLoan Services; BPAS Trust Company of Puerto Rico; Hand Benefits & Trust; Healthcare Consulting Services; VEBA and Health & Welfare Services; Healthcare Consulting Services, NRS Trust Administration, and Global Trust Company.

BPAS maintains offices in Utica, Syracuse, Rochester, and New York City (New York); East Hanover (New Jersey); Pittsburgh and Philadelphia (Pennsylvania); Houston (Texas); Woburn (Massachusetts); Sioux Falls, (South Dakota); Bloomington (Minnesota); and San Juan, Puerto Rico. The organization provides administration services to approximately 4,200 plans throughout the U.S. and Puerto Rico. BPAS Plan and Recordkeeping Services provides design consulting, document preparation, and administrative services to sponsors of defined contribution type plans. BPAS's daily valuation system serves in the dual capacity of a participant record keeping system and a trust accounting system. As such, BPAS's daily valuation system is performing both BPAS Plan Administration and Recordkeeping functions, HB&T custody functions, and BPAS Trust Company of Puerto Rico custody functions through a series of seamless and integrated transactions.

Please see below for a summary of the acquisitions that CBSI and BPAS have completed over the years:

- On July 31, 2003, BPAS acquired the assets and business of a Syracuse-based defined benefit and health and welfare practice from Pricewaterhouse Coopers, LLP. Harbridge Consulting Group (now BPAS Actuarial & Pension Services and BPAS Healthcare Consulting Services) provides actuarial and health and welfare consulting services.
- On May 18, 2007, BPAS completed its acquisition of Hand Benefits & Trust, Inc. (HB&T), a Houston, Texas-based provider of employee benefit plan administration and trust services. HB&T provides employee benefit trust services for approximately 21.5 billion in assets. BPAS, LLC performs trust operation services pursuant to intercompany agreements for mutual client plans of HB&T or BPAS Trust Company of Puerto Rico. HB&T also administers sub-advised Collective Investment Funds (CIF).
- On July 7, 2008, BPAS acquired the assets and business of the Philadelphia office of Alliance Benefit Group (ABG) MidAtlantic from BenefitStreet, Inc. ABG was a provider of defined contribution plan administration services, actuarial services and investment advisory services.
- On November 4, 2011, BPAS acquired a license from Access Control Advantage, Inc. to offer "Non-traditional Retirement Loan Product, Service or Process" for employee benefit plan loans. The product was renamed to MyPlanLoan (MPL). MPL focuses on offering loan continuation services to terminated retirement plan participants in an effort to help them avoid having to default on their loans.
- On November 30, 2011, BPAS acquired certain assets and liabilities of CAI Benefits Inc., a provider of defined contribution TPA services, actuarial services and healthcare consulting services.
- In December 2013, BPAS reached an agreement to acquire from EBS-RMSCO, Inc., a subsidiary of The Lifetime Healthcare Companies, its professional services practice that provides actuarial valuation services to clients who sponsor pension and post-retirement medical and welfare plans.

- In June 2015, BPAS acquired the Plan Administration and Recordkeeping practice of Lifetime Benefit Solutions (LBS), a subsidiary of Lifetime HealthCare Company. This conversion included approximately 60 plans serviced in conjunction with 21 financial intermediary partners, many of which were new relationships for BPAS.
- On February 3, 2017, Community Bank System, Inc. acquired Northeast Retirement Services, Inc. (NRS) and designated the Company a subsidiary of BPAS. NRS and its subsidiary Global Trust Company are based in Woburn, Massachusetts, and provide fund of fund, custom target date and collective investment trust administration, transfer agency, and retirement plan administration services. As of the date of the transaction, the combined BPAS/NRS entity provides trust services to over \$50 billion in plan assets.
- In July 2021, Community Bank System, Inc. has acquired Fringe Benefits Design, a Bloomington, Minnesota-based provider of retirement plan administration and benefits consulting services. Fringe Benefits Design is a subsidiary of BPAS. The move gives it 510,000 retirement plan participation accounts and \$110 billion of total assets in trust.

## Scope of Report

Benefit Plan Administrative Services, Inc. (BPAS or Company or organization or organization), a wholly owned subsidiary of Community Bank System, Inc., is comprised of 12 lines of business:

- **BPAS Plan Administration & Recordkeeping Services (PARK):** Bundled administration, recordkeeping, and custody for defined contribution-type plans and all types of IRAs.
- **IRA Services** – Part of PARK, this group supports a range of IRAs (Auto Rollovers, traditional and Roth IRAs as rollover options, IRA Rewards and more)
- **MyPlanLoan** – Part of PARK, this group provides non-payroll deducted loan administration to participants of BPAS and certain other partners
- **BPAS TPA Services** – Part of PARK, this group provides unbundled retirement plan services in support of balance forward and third-party recordkeeping plans.
- **BPAS VEBA and Health & Welfare services** – Part of PARK, this group provides administration of Funded HRA Accounts held in VEBA or Section 115 Trusts, Notional HRA Accounts, Flexible Spending Accounts, Health Savings Accounts, Parking / Transit programs, COBRA and certain other services, either on a direct basis or in partnership with outside TPAs
- **BPAS Actuarial & Pension Services** (formerly Harbridge Consulting Group): Actuarial and consulting services for traditional defined benefit, cash balance, executive supplemental retirement and other post-retirement benefits, including retiree medical.
- **BPAS Healthcare Consulting Services:** Plan design, actuarial consulting, RFP and analysis, and contracting with service providers in select markets.
- **BPAS Fiduciary Services:** ERISA 3(38) fiduciary services for employee benefit plans of BPAS and select outside partners, as well as participant education services.
- **BPAS Trust Company of Puerto Rico:** Custody and Directed trustee services for PR 1081 plans administered by BPAS Plan Administration and Recordkeeping Services.
- **Hand Benefits & Trust, a BPAS Company (HB&T):** Institutional Trust services, including Collective Investment Fund administration and custody for non-Puerto Rico plans administered by BPAS Plan Administration and Recordkeeping Services, and certain other institutional services
- **NRS Trust Administration:** Institutional transfer agency, target date administration, trust product administration, and certain other institutional trust services (non-fiduciary in nature).
- **Global Trust Company:** Directed and discretionary trustee services and expertise for Collective Investment Trusts and Institutional trust products (fiduciary in nature).

This report addresses the relevant controls surrounding BPAS Plan Administration & Recordkeeping Services including Custodial Services related thereto, BPAS Actuarial & Pension Services, BPAS VEBA and Health & Welfare Services, BPAS AutoRollovers and MyPlanLoan (Part of Plan Administration and Recordkeeping). Custodial activities provided by Hand Benefits & Trust Company and BPAS Trust Company of Puerto Rico for plans administered by BPAS Plan Administration and Recordkeeping Services are also included within the scope of this report. Separate SOC Reports are issued for HB&T activities supported by the AddVantage Trust System and for NRS and Global Trust Company activities supported by the IS System, and as such, the key controls for these activities are not covered in this report.

BPAS's customers include any organization that has contracted with BPAS to provide Defined Contribution, Defined Benefit, Individual Retirement Account (IRA), Voluntary Employees Beneficiary Association (VEBA), Health Reimbursement Arrangement (HRA), Health Savings Account (HSA), Flexible Spending Account (FSA), COBRA Administration and nonqualified deferred compensation retirement products and services. The activities of Community Bank N.A. (CBNA), Hand Securities Inc. (HSI), Northeast Retirement Services (NRS), Global Trust Company (GTC), and Community Bank System, Inc. (CBSI) are beyond the scope of this report. Additionally, this report does not include the controls or control objectives of the sub-service organizations utilized by BPAS, as further described later in Section III.

## Key Systems for the Plan Administration and Recordkeeping Service

BPAS utilizes various IT systems throughout its operations to perform all administration, valuation, and transaction processing functions. The following is an overview of the key application systems that make up the Plan Administration and Recordkeeping Service:

### OmniDC

The OmniDC application is the primary recordkeeping system used to administer certain types of defined contribution, health and welfare plans, and all daily valuation plans at BPAS. The system manages all plan sponsor and participant transactions, providing a high level of automation in managing contribution and trading transactions, benefit disbursements, and compliance with the Internal Revenue Code (IRC). OmniDC was purchased from SunGard Corporation.

### Plan and Task Manager

Plan and Task Manager (PTM) is a proprietary workflow and contact management system that tracks completion dates for all tasks performed by BPAS employees, as well as a sophisticated client contact and plan management tool. PTM interfaces with the OmniDC and CensusPro applications to manage benefit transaction processing. BPAS, Inc. utilizes The PCA Group to assist with the development and maintenance of the PTM application.

### Delta Data

Delta Data includes four applications, Fundlinx, Trade Manager, Position Manager, and Revenue Manager. The Trade Management system pushes, and tracks trades processed from the OmniDC recordkeeping system to the National Security Clearing Corporation ("NSCC"), including confirmation and settlement of the trades at each underlying fund family. The Position and Revenue Manager modules perform fund position reconciliation and fund revenue tracking. Fundlinx is utilized for fund research and information. The system also aggregates all individual mutual fund and company stock transactions for daily valuation plans into net trading positions.

### Wex Health

The Wex Health system receives balance information from Omni on a nightly basis. These balances are used to populate participant accounts and debit cards used for health claims.

### DB Precision

BPAS Actuarial and Pension Services uses DB Precision as a recordkeeping system and plan sponsor/participant online platform for defined benefit administration.

## Ancillary Tools and Systems

The following is an overview of other ancillary systems and tools that are used in delivering the Plan Administration and Recordkeeping Service.

### **1099 Express**

1099 Express was purchased during 2010 and is used to generate 1099Rs, 1099 Misc., W2s, and 5498s.

### **ASC**

ASC is an application used to allocate employer year-end contributions and forfeitures and perform non-discrimination tests under IRC Sections 401(a)(4), 401(k), 401(m), 410(b), 414(s), and 1081.01(d) under the Internal Revenue Code of Puerto Rico.

### **CensusPro (CensusPRO™)**

CensusPro is a web-based application system used by plan sponsors to communicate periodic participant census data. CensusPro is a proprietary system, designed internally and developed utilizing the software engineering expertise of The PCA Group, Inc. (PCA) based in Buffalo, New York, for system development and maintenance. CensusPro directly interfaces with the OmniDC and Task Manager applications for administering contribution transactions.

### **CensusPro2 (FIS DVW)**

CensusPro2 is a web-based application system used by plan sponsors to communicate periodic participant census data. CensusPro2 is the Data Validation Web (DVW) application which was purchased from FIS. BPAS is in the process of migrating plans off of CensusPro and onto CensusPro2.

### **Funds Available**

Funds available tracks contribution, loan, and participant rollover money received at a plan level, as well as the date the dollars are traded. The resulting balance of any money received less money traded is the "Funds available" to trade balance for each plan.

### **Visual AccountMate**

Visual AccountMate (VAM) is an accounting system used primarily for billing and accounts receivable administration, and as a "shadow booking" system of the parent company's accounting system. The application was purchased from Accountmate Software Corporation.

### **DBVAL**

BPAS Actuarial and Pension Services uses DBVAL as a valuation system, which determines pension plan liabilities for government reporting and plan sponsor accounting purposes. This system was in place until January 2021.

### **OPEVs**

BPAS Actuarial and Pension Services uses OPEVs as a valuation system, which determines other post-employment benefit plan liabilities for plan sponsor accounting purposes. This system was in place until January 2021.

### **Proval**

BPAS Actuarial and Pension Services uses Proval as a valuation system, which determines pension plan liabilities for government reporting and plan sponsor accounting purposes and other post-employment benefit plan liabilities for plan sponsor accounting purposes.

### **PayPilot**

PayPilot is an application that is used to generate and track distribution and loan checks.

---

**PRSoft**

PRSoft's PRPay module is utilized to generate Puerto Rican 480.7C forms. PRPay was not included within the scope of this report.

**ftwilliam.com 5500 Forms, Plan Documents**

BPAS Plan Administration and Recordkeeping Services, BPAS TPA Services, and BPAS Actuarial and Pension Services use the ftwilliam.com 5500 Forms application for web-based e-filing services and plan documents. This application was not included within the scope of this report.

## Relevant Aspects of the Control Environment, Risk Assessment, Monitoring, Management Oversight, and Governance

**Control Objective 1: Controls provide reasonable assurance that the overall management and governance structure is established and implemented by the organization.**

An organization's control environment reflects the position, attitude and awareness of its directors, management and employees concerning the importance of internal controls and the emphasis given to adherence to the Company's policies, procedures, methods and organizational structure. The following is a description of the key elements of the control environment as it pertains to BPAS.

The elements of the control environment include:

1. Integrity and Ethical Values
2. Assignment of Authority and Responsibility
3. BPAS's Organizational Structure
4. Human Resources Policies and Practices
5. Risk Assessment
6. Information and Communication
7. Monitoring
  - a. Segregation of Duties
  - b. Internal Audit
  - c. Regulatory Oversight

### Integrity and Ethical Values

Maintaining a culture that demands integrity and ethical values is critical to the establishment and maintenance of an effectively controlled organization. BPAS has programs and policies designed to promote integrity and ethical values within the Organization. The foundation of BPAS's control environment is driven by the Organization's core values, which include, but are not limited to, the highest levels of integrity and respect for all individuals, as well as continuous quality and exceptional customer service. These core values are complimented by the Company's customer-driven philosophy.

### Assignment of Authority and Responsibility

The control environment is greatly influenced by the extent to which individuals recognize that they will be held accountable. This holds true throughout the Company, from staff personnel up to Executive Management, who have ultimate responsibility for all activities within the entity, including internal control. The extent of accountability includes assignment of authority and responsibility for operating activities and the establishment of reporting relationships and authorization protocols. BPAS encourages individuals and teams to take the initiative in addressing issues and resolving discrepancies. Policies describing acceptable business practices and the knowledge and experience of key personnel and resources are communicated throughout the Company. These policies provide the framework for employees to carry out their responsibilities and duties.

### BPAS's Organizational Structure

The Company's organizational structure provides an overall framework for strategically planning, directing, and controlling operations. The operating structure directly relates to controls over the daily execution of transactions, services, and operations. The organizational structure assigns authority and responsibility within the Company to provide for adequate staffing, segregation of duties, efficiency of operations, and adequate concentration of knowledge and skills. The structure also facilitates oversight of operating activities. BPAS activities are overseen by the Board of Directors of BPAS and CBSI. BPAS's organization chart is summarized below:



BPAS is organized into eight primary departments that are listed below, each with a Unit Manager and Senior Staff Member to oversee underlying department subgroups. It's important to note that both Technology Services and Information Security are associated with the parent company CBSI, however both maintain consistent focus on BPAS operations and security controls.

1. Finance
  - a. Accounting
  - b. Office Management
2. Defined Contribution Plan Administration and Recordkeeping
  - a. Document Services
  - b. Consulting /Defined Contribution Administration
  - c. Plan Compliance
  - d. Conversion Unit
  - e. Daily Valuation Operations
  - f. Applications Programming
  - g. Mutual Fund Services
  - h. Defined Contribution Plan Recordkeeping
  - i. Participant Services
  - j. MyPlanLoan
  - k. Auto Rollovers
3. Actuarial and Pension Services/Healthcare Consulting
  - a. Large Plan Services
  - b. Small Plan Services
  - c. Healthcare Consulting
4. VEBA and Health & Welfare Administration
5. Business Analyst
6. Technology Services
  - a. Systems Admin
  - b. Systems Analysis
  - c. Telecommunications
  - d. Network Security
  - e. Technology Support
7. Information Security
8. Sales and Relationship Management

The departments, functional areas, and the reporting lines associated with each are documented in an organization chart (Control 1.5). Responsibilities are allocated among departments and personnel so as to segregate the input, processing, disbursement, and monitoring functions (Reference the Segregation of Duties subsection below).

## Human Resources Policies and Practices

The Organization has policies and procedures for controlling the hiring and termination of employment. Checklists are completed by the Human Resources department when new employees are hired. When employees leave the Organization, a change form is completed. All prospective employees are interviewed by Management. Hiring policies also include requiring the candidate to have obtained a minimum level of education and experience for the position, pre-employment tests, and management's completion of reference and background checks.

Training of personnel is accomplished through supervised on-the-job-training, seminars, and regular in-house educational courses. All employees are required to complete an examination in basic retirement plan administration within the first year of employment. In addition, Plan Consultants are required to complete a certification program sponsored by a professional association, including the American Society of Pension

Professionals & Actuaries (ASPPA). Managers are also required to conduct regular in-house training sessions so that all personnel are informed about changes in systems and tax regulations.

Employees who are hired under the Actuarial Student Program are expected to make steady progress toward the completion of designations under the Society of Actuaries and/or the Joint Board for enrollment of actuaries.

Employees are required to acknowledge their agreement to the Company Code of Conduct and to the policies defined within the Employee Handbook upon hire (Control 1.2).

The Human Resources department issues job descriptions to all new hires in conjunction with the hiring process. Job descriptions include a description of the position's roles and responsibilities (Control 1.4).

Formal performance reviews are conducted as needed after 30, 90, and 180 days for new employees, and on an annual basis after one year of service. Employees are evaluated on objective criteria based on performance, and an overall rating is assigned. The evaluation of those employees rated less than satisfactory are reviewed to determine the necessary actions to improve performance.

The Organization has a formal code of conduct, which, among other things, establishes rules of conduct for all employees. Specifically, employees are prohibited from divulging confidential information regarding customer affairs.

## Risk Management

BPAS recognizes that risk management is a critical component of its control environment and operations. The Company's ability to identify, measure, monitor, and report risk is critical to its soundness and profitability. To manage corporate assets and to serve customers as expected, CBSI's Internal Audit department conducts a formal risk assessment on an annual basis.

The Organization maintains insurance coverage against major risks. Coverage includes professional services, trust services, as well as other business liabilities. Coverage is provided by 10 insurance companies, which are considered by senior management of CBSI to be financially sound. Amounts of coverage are carried at levels that senior management and the Board of Directors of CBSI believe is reasonable given the size and scope of BPAS's operations.

## Information and Communication

BPAS has implemented various operational procedures to facilitate communication so that all employees understand their individual roles and responsibilities over transaction processing and controls, and to so that significant events are communicated in a timely manner. These methods include orientation and training programs for newly hired employees, quarterly firm-wide communications that summarizes significant events and changes occurring during the quarter, and the use of electronic mail messages to communicate time-sensitive messages and information.

Executive management and corporate leadership hold periodic meetings to provide insight into strategic direction, key decisions, and earnings results. Managers also hold periodic staff meetings, as appropriate. Every employee has a written position description, and the BPAS Employee Handbook includes the responsibility to communicate significant issues and exceptions to a higher level of authority within the Organization in a timely manner.

## Monitoring

CBSI maintains an Audit Committee that provides oversight and is responsible for the development of the Organization's risk management and security programs, the Internal Audit Department, the relationship with the external auditor, and the review and approval of risk management related policies and procedures.

Management and supervisory personnel monitor performance, quality and the operation of controls as a normal part of their activities. A formal management information and reporting system exists which permits monitoring by management of key control and performance measurements. All required functions for plan administration and recordkeeping are entered into a computerized tracking system, which lists tasks, unit responsibilities and priority status.

Every other week, BPAS management meets and discusses the organization's operations, including risks facing the organization and its information systems (Control 1.3).

### a. Segregation of Duties

Activities are conducted in accordance with written policies and procedures to facilitate monitoring throughout the Organization operations and transaction processing. Policies and procedures are periodically reviewed and updated for ongoing applicability. In addition, procedure responsibilities are allocated among personnel so as to segregate the following functions within the transaction processing cycles:

- Plan documents and implementation;
- Input of contribution transactions and trading;
- Distribution and/or loan processing;
- Reconciliation activities;
- Plan administration, consulting, and compliance monitoring; and
- Management Control.

### b. Internal Audit

The Company's Internal Audit function provides the Audit Committee, executive and senior business management and regulators with an independent assessment of the Company's ability to manage and control its risks. BPAS's activities are subjected to a continual internal audit program. Audits are conducted by CBSI's Audit Department and are scheduled based on formal risk ratings. The Internal Audit Department is under the general supervision of the Audit Committee of CBSI's Board of Directors and has unrestricted access to all functional areas within BPAS.

The activities of the Internal Audit Department are conducted in accordance with an audit plan, which is approved by the Audit Committee. The audit plan is developed with consideration given to regulatory factors, prior audit results, external audit findings, risk exposure and input from relevant members of management. The audit program is designed to evaluate compliance with policies, procedures, applicable laws and regulations to which BPAS and its customers are subject.

The Audit Committee meets periodically to monitor progress compared to the audit plan. Upon the completion of an audit, an internal control rating is assigned based on qualitative measures of internal controls and the effectiveness of the Organization's operations. Audit findings are documented in formal written reports that are submitted to members of management and the Audit Committee. Management is then required to submit, within a specified period of time, a written response that discusses the intended resolution of reported items.

The Internal Audit Department within CBSI also assists in the development and implementation of policies and procedures. Upon the implementation of new policies and procedures or changes to existing policies and procedures, the Internal Audit Department performs certification procedures to evaluate if policies and procedures have been implemented. See Section V: Other Information Provided by Benefit Plan Administrative Services, Inc. for a list of audits and reviews that are performed over BPAS entities and operations.

### c. Regulatory Oversight

BPAS, as a subsidiary of CBSI, is subject to regulation by the Federal Reserve, Texas Department of Banking, PR Commissioner of Financial Institutions, FINRA, Department of Labor and SEC. As such, BPAS and its subsidiaries are required to file periodic reports and are subject to periodic examinations.

## Description of Controls

Controls surrounding the Plan Administration and Recordkeeping Service pertain to the Organization's ability to safeguard and manage the assets of individuals and user entities in an organized, authorized, and controlled manner, to prevent the loss of assets and information held in trust, and to prevent unauthorized access to sensitive information. These controls operate over the receipt, management, and distribution of the assets. If suitably designed and operating effectively, these controls will limit the opportunities for fraud and incorrect processing, reducing the risk exposure of the Company and its clients.

The following describes the processes, procedures and controls surrounding BPAS's Plan Administration and Recordkeeping Service:

1. Defined Contribution Benefit Plan Administration, VEBA and Health & Welfare Administration, and Transaction Processing Systems
  - a. OmniDC
  - b. 1099 Express
  - c. ASC
  - d. CensusPro
  - e. CensusPro2
  - f. Plan and Task Manager (PTM)
  - g. Funds Available
  - h. Visual AccountMate
  - i. Delta Data
  - j. ftwilliam.com 5500 Forms
  - k. Wex Health
  - l. PayPilot
  - m. PRSoft
2. Defined Contribution Benefit Plan Administration and Reporting
  - a. New Plan Account Administration
  - b. Plan Changes and Terminations
  - c. Participant Administration
  - d. Census Reporting
  - e. Recordkeeping Transaction Processing
  - f. Voice Response Unit (VRU) and BPAS Online Transactions
  - g. Distribution Processing
  - h. Valuation Reports and Trust Accounting
  - i. Collection of Income and Fee Assessment
  - j. Claims Payment
  - k. IRS, PR Hacienda and ERISA Compliance
3. Actuarial Valuation and Defined Benefit Administration Systems
  - a. DB Precision
  - b. ftwilliam.com 5500 Forms
  - c. DBVAL
  - d. OPEVs
  - e. Proval
4. Actuarial Valuation and Defined Benefit Administration
  - a. Benefit Administration
  - b. Census and Financial Information Collection
  - c. Valuation Reports
  - d. Government Reporting

## Benefit Administration and Transaction Processing

**Control Objective 2: Controls provide reasonable assurance that new plan sponsors, plan participants, and participant loans are authorized and approved and then processed completely and accurately.**

### **New Plan Account Administration**

BPAS establishes all new plans following formal processes and procedures. All prospective plans are reviewed by the New Account Review Committee prior to being accepted by BPAS and initiation of the implementation process. Accounts are initiated when a plan sponsor requests service and executes the agreements to retain BPAS to provide such services. If a plan sponsor has a direct contractual relationship with BPAS, an OFAC (Office of Foreign Assets Control) scan is performed to verify that the company is not on any of the government watch lists (Control 2.1).

BPAS requires the completion of a Service Agreement that outlines the services to be performed, each party's responsibilities, and administrative fees of each party prior to BPAS performing services for the plan (Control 2.2). Due to the time frame for plan conversion, there are certain services that may be initiated prior to the execution of the service agreement such as plan document services and some services to establish the plan and participant accounts on the BPAS platform. The Administrative Service Agreement is required for all recordkeeping and Custodial Services. Daily valuation clients that engage HB&T or BPAS Trust Company of PR to serve as Directed Trustee or Custodian also execute a Directed Trustee or Custodian Agreement. New plan sponsors, financial intermediaries, and BPAS sales associates are required to complete the BPAS Installation Kit to capture the necessary information required to establish the new plan at BPAS (Control 2.3). A New Account Checklist is completed by BPAS to document the implementation process (Control 2.4).

New plans are established in the PTM application, and a Consultant is assigned to administer the Plan once all plan information has been obtained and the New Account Checklist is completed (Control 2.5). A "Pre-Hand-off Meeting" is held with each department within BPAS that will be involved with establishing and servicing the new plan.

An Implementation Specialist is assigned to manage the conversion process. BPAS provides plan sponsors with various tools for the conversion process such as authorizations for fund transfer and census file specifications to permit accurate contribution processing.

After the pre-hand-off meeting, the Conversion Specialist assigned to the conversion begins working with the plan sponsor, prior administrator, and party that holds assets to determine the timeframe for the conversion. Once this timeframe is established, the timeframe is communicated to the plan sponsor and financial intermediary. A Conversion Checklist is completed by the Conversion Manager to evaluate the completeness of the conversion process for new plans. (Control 2.8). The Conversion Team reviews the information provided by the plan sponsor and generates a summary document out of Omni to determine if participant information items such as eligibility, vesting, methods of allocation and other pertinent provisions were completed and Plan Consultant performs a secondary review (Control 2.6).

BPAS does not accept funds from prior benefit administration and processing service providers until receipt of all conversion documentation. A Plan Consultant reviews the information provided by the plan sponsor and reviews a "scrubber" to determine if participant information items such as eligibility, vesting, methods of allocation, and other pertinent provisions are correctly entered into the system. To determine if plan assets are recorded, the BPAS Conversion Team reconciles the plan assets and enters the information into the OmniDC accounting system. A Conversion Specialist, working in conjunction with the Plan Consultant, reviews all plan documents and evaluates if the plan is coded into the system by reviewing the "DECON PACK," which compares the new data coded into the system with the data provided by the plan sponsor (Control 2.7).

Qualified employee additions to existing plans are communicated when participant information is received through census data communicated from the plan sponsor. The submitted participant addition is then uploaded into OmniDC during the contribution processing cycle (Control 2.9).

Plan participants complete a Standard Investment Election Form that is communicated to BPAS for transaction processing. Transactions are then entered by a Processor and independently reviewed by another Processor (Control 2.10).

Traditional participant loans are requested through the completion of a standard Loan Request Form. All requests are reviewed by a Participant Services Representative or a Distribution Specialist to determine if they were accurately completed and then entered within BPAS systems (Control 2.11). Participant loans through the MyPlanLoan program are requested and automatically permitted based on plan terms through the BPAS website (Control 2.12).

During 2005, BPAS began offering the ReservePlus Loan program, which is now known as MyPlanLoan (MPL), to its clients. Participants within plans that have adopted the program may apply for a loan via BPAS's web portal. The participant receives a monthly statement reporting the loan balance, minimum payment due and a summary of the previous month's transactions. Loan payments are submitted to MPL and forwarded to the plan custodian. MPL also transmits information to the recordkeeper regarding loans to be defaulted due to insufficient or untimely payments.

## Participant Plan Changes

**Control Objective 3: Controls provide reasonable assurance that changes to existing plans and participant records are authorized.**

BPAS requires written authorization from plan sponsors for any material changes in plan design. Plan Consultants review the terms of applicable documents of client accounts when legal changes and/or plan amendments occur. All plan amendments are signed by the client and maintained for confirmation. Plan documents and amendments are prepared by the Document Services Team (Control 3.1).

A Fund Change Form and other documentation for the change are provided to the Sales Relationship Manager for review and are used to update BPAS's recordkeeping systems.

BPAS requires written authorization from the plan sponsor to terminate or close an account (Control 3.4). Authorization is maintained in the account file and is reported to Senior Management on a monthly basis. Participant terminations are communicated when census data is received from plan sponsors and these participant termination requests are then processed within the OmniDC system (Control 3.3).

## Voice Response Unit and BPAS Online Transactions

Participants with plans using OmniDC can execute transfers between funds within the plan by accessing the BPAS voice response unit (VRU) or over the Internet. The VRU and web portal provide additional means for participants and plan sponsors to communicate transactions for daily valuation plans. Transactions requested through the BPAS Voice Response Unit (VRU) and the BPAS web site can only be processed if a Participant Identification Number (PIN) is entered into the system. (Control 3.2). VRU PINs are issued by the OmniDC Unit, and letters of confirmation are sent to plan participants the first business day following any transactions executed through the system. The system forces participants to change their PINs upon initial login.

Participants use a username and password to access the web portal. Registration to access the web portal is performed online through the BPAS website. Participants are required to create an alternate user account and change their passwords upon initial login. Instructions on the allocation of participant's accounts are captured through the VRU and the web portal and are then processed in the OmniDC application. Batch jobs run daily to transfer participant records and transaction information to the OmniDC system for processing.



## Participant Deferrals and Contributions

**Control Objective 4: Controls provide reasonable assurance that participant deferrals are accounted for and contributions to employee benefit plans are processed completely and accurately.**

New employees are communicated by the plan sponsor through census data. Once eligible, new employees are required to communicate their investment elections via one of three methods: a standard hardcopy Investment Election Form, the BPAS web portal system, or through its Voice Response Unit (VRU). Contributions provided for participants who have not specified their investment elections are automatically invested in the plan's default investment fund. Manual elections are entered by a processor and independently reviewed by another processor. Census data received electronically is automatically validated by the CensusPro (CPRO) application during the upload process.

CensusPro requires the correction of file format errors by the plan sponsor prior to permitting the file to be uploaded for processing (Control 4.1). Daily, CPRO reports are automatically generated that summarize if census data files successfully uploaded to the BPAS web servers (Control 4.2). BPAS Census Processors monitor CPRO reports to confirm the census data files uploaded to the BPAS web servers by Plan Sponsors via CensusPro for processing.

The OmniDC application prevents contributing participant deferrals and/or employer contributions to funds not authorized for investment by plan sponsors (Control 4.3). Additionally, plan eligibility requirements by contribution source are defined within the OmniDC application, which prevents non-qualified employees from contributing until all plan requirements have been achieved to become a valid participant (Control 4.4).

A Plan Administration Checklist is completed by the Plan Consultant to document the year-end employer allocations and required discrimination testing performed by BPAS in accordance with plan terms (Control 4.5).

BPAS maintains all daily valuation assets in super-omnibus or plan level omnibus accounts within mutual funds. Fund transactions are accumulated from participant and plan sponsor instructions, and then traded on a net basis. All fund transactions are reconciled to plans. Daily, transactions entered into the OmniDC system are compared to the Net Trade Recap Report to assess the accuracy of the contribution information that was entered and processed. (Control 4.6).

### Census Reporting

All census gathering activities are coordinated by the census unit. BPAS primarily accepts census information using two methods:

1. Where clients use a payroll service bureau, BPAS arranges to have relevant data transmitted directly from those service bureaus to BPAS in a standard format. The information is uploaded directly into CensusPro or CensusPro2 and then BPAS plan administration system.
2. The census data may be manually entered or uploaded and transmitted through BPAS's web-based reporting systems, CensusPro or CensusPro2.

For daily valuation plans, contribution data reported to BPAS is processed in "edit" mode within the OmniDC system to verify that contributions are being reported for eligible plan participants. Processing performs a number of checks and validations, including, but not limited to, required age and service requirements and loan payments. Contributions or participants who have not met the required age and service requirements as set forth by the plan and documented in the summary plan description or who have terminated employment with the employer, and loan payments for loans that have already been discharged are rejected. BPAS will resolve any transaction that has been rejected in edit mode before it proceeds with the processing of a contribution file. Contribution information on file without rejected transactions is communicated back to the client electronically in the form of a trade verification. The custodian for all daily valuation plans is HB&T. All sub-custodial services for BPAS's daily valuation plans are performed at BPAS's offices by dual employees (employed by both BPAS and CBNA).

Participant additions, changes, and terminations are communicated through census data. CensusPro/CensusPro2 processes these changes and communicates them to the OmniDC application, which is updated automatically.

## Trade Processing

### **Control Objective 5: Controls provide reasonable assurance that trades are recorded completely and accurately.**

BPAS utilizes a comprehensive tasking approach to retirement plan administration. BPAS maintains several departments wherein tasks to service a plan are performed by a number of employees at different stations and levels. All transactions for daily valuation plans are processed within the OmniDC application. OmniDC processes participant contributions according to participants' defined allocations to the funds specified by the plan. The system processes the contributions considering applicable IRC requirements, including participants' maximum allowable contributions, withholding taxes for disbursements, as well as other restrictions. OmniDC also processes transactions following defined plan specifications, such as age and employment history requirements, and plan eligibility by contribution source, which prevents non-qualified employees from contributing until all requirements have been achieved to become a valid participant.

Contribution and distribution transactions to be traded are flagged with a system status of "PROCESSED" in the Plan and Task Manager (PTM) application. A batch process is executed at the end of each day to identify these transactions in the OMNIDC application and updates their system status from "EDIT" to "PROD". Once these distribution and contribution transactions are completed, the system status is updated to "SUCCESSFUL" (Control 5.1). The Distribution and Contribution Team verifies that all reported "Successful". All transactions must be successful prior to trading in order to be included in the nightly trade job. If an "Unsuccessful" response is received, processors will review the detail in the OmniDC application as well as the related detail in the PTM application to determine why that transaction resulted in an error. Any differences are corrected, and the comparison is run again. Processors perform key word searches just before trading to determine if all transactions are being processed appropriately.

Prices for mutual funds and securities to be traded are obtained from authorized sources, including the National Securities Clearing Corporation (NSCC). Pricing files are continuously loaded into OmniDC as received. Automated processes determine the point at which all prices required for nightly trading have been obtained. If there are prices that are not available on a particular night, the trader has the ability to start the trade process. Transactions that require prices that are not available are placed in a system status of "HOLD" and will not be processed that evening (Control 5.2). An OMNI Programmer is available for system support during the nightly trade process. Securities/Mutual Funds where pricing cannot be obtained remain on HOLD status in OmniDC and are monitored to be processed once obtained, typically the next business day.

Throughout transaction trade processing, OmniDC Unit Processors must sign-off on the "Trading Checklist," confirming each step completed. The Trading Checklist is completed daily during the preparation of the trade Order files. Daily, the "Trading Checklist" is completed during the preparation of the trade Order files. The checklist includes a requirement for reviewing and reconciling the total trades and dollar totals from the Order file. (Control 5.3).

The OmniDC Unit also generates participant and plan level reports, allocates dividends, and processes fees payable from plan assets.

BPAS uses Delta Data Position Manager to monitor the investment positions maintained in the OmniDC system with the fund positions from NSCC and the application's history of trading transactions that have been executed to verify asset values and the completeness and accuracy of initiated trades. Positions that are not in agreement are investigated and corrected on a daily basis.



Mutual Fund Dividend information is received electronically from the NSCC. Trial dividend posting in OmniDC are performed by members of the Daily Processing Unit to confirm that the shares that will be posted to OmniDC match what actually posted at the fund. If the shares match, the dividend is processed. If the trial post results in an inaccurate number of dividend shares posted, reconciliation is performed to determine if adjusting transactions are required.

Claims cannot be processed until the status of the claim is changed to indicate that documentation was attached for the claim.

For Balance Forward Plans, BPAS relies on third-party information for the valuation of assets. Plan Consultants reconcile information received. The reconciliation is reviewed by a senior staff member. If the information is questionable, the client is contacted for additional information or clarification.

Plans with more than 100 participants must provide an Independent Auditors' Report regarding the plan assets.

## Participant Disbursements and Payments

**Control Objective 6: Controls provide reasonable assurance that disbursements and payments to participants are authorized and remitted completely and accurately.**

Participant Service Representatives or Distribution Specialists review disbursement requests to evaluate if all required paperwork and authorizations were completed. (Control 6.1). Disbursement transactions are then entered into the OmniDC system for processing. During 2020 BPAS implemented a new e-signature (paperless) option for distribution requests, which is available for a limited number of plans and only for terminated participants meeting certain criteria, including having a vested balance under \$20,000. Disbursements are allocated in the OmniDC application in accordance with plan parameters to determine if distributions are accurately charged to the appropriate participant in the plan and against the assets held by the plan for the participant.

Segregation of duties exists between the authorization, distribution, and recording of disbursements. A Plan Consultant or a Distributions Specialist approves disbursement requests, and a task is created for the Distribution Unit. Disbursement checks are independently processed in the Trust Operations Department.

Check stock is maintained in a locked safe that can only be accessed by authorized individuals. The safe combination is split between two individuals, requiring each person to enter a portion of the code to gain access to the check stock.

A check log is maintained to record the first and last check numbers processed for distribution. Check processing is performed by the Trust Department, who are independent from the benefit administration and contribution processing functions.

Requests for disbursement paperwork from terminated participants are processed through the BPAS web portal. Electronic requests create print jobs with forms specific to each plan, which are required before processing. The forms may either be printed by the participant or mailed to participants' home addresses with instructions to complete and return them to BPAS. Terminating participants that are requesting a final distribution must complete the required forms and return them to BPAS prior to disbursement. (Control 6.2). Returned forms are reviewed by the Plan Consultant or a Participant Services Representative; if a transaction is approved, a task is posted in PTM. Once the required forms are received, distributions are processed from the OmniDC system. A distribution log is sent to the Trust Operations unit at BPAS, which processes all checks. For non-daily valuation plans, a transmittal letter is sent to the trustees or broker with instructions on each distribution.

If a terminated participant meets the requirements to request a distribution completely on-line, without having to complete a paper application, the participant will see the paperless option on the participant website. If the participant selects that option, he will need to successfully answer security questions to confirm his identity and acknowledge review of the disclosures and special tax notice before submitting the

request. The distribution and the PTM task are set up during the nightly trading cycled and reviewed the following business day before the liquidation is processed. The distribution is included in the check log used by the Trust Operations unit at BPAS, which processes all checks.

BPAS receives funds to cover contributions, loan payments, and rollovers. After Wire Authorization Forms are prepared, on a daily basis, a Summary Trade Order report illustrating plan investment transactions is prepared by a BPAS Trust Operations employee to verify the total dollar amount and accuracy of the disbursements. The report is then reviewed by an independent Trust Operations employee prior to faxing the request to the Wire Desk for execution (Control 6.3). Notifications from the Wire Room indicate when funds have been received and/or transferred. The wire transfers are confirmed with BPAS, and a BPAS Trust Employee confirms that all wire requests have been executed. BPAS authorizes all outgoing wire transfers of funds by notifying the Wire Room. The Wire Room subsequently confirms that the funds have moved according to BPAS's authorization. Confirmations from the Wire Room are then verified for accuracy by the Trust Unit.

BPAS completes a Wire Procedure Checklist each day to verify the daily trading activity and authorization of wire transfers of funds. The Wire Procedure Checklist is independently reviewed for confirmation (Control 6.4).

## Customer Statements

**Control Objective 7: Controls provide reasonable assurance that statements provided to participants and plan administrators are complete and accurate.**

For defined contribution plans, the annual reports are posted on BPAS's Sponsor Website. Reports include an annual summary of participant statements, a trust asset report, detail of participant balances, loan and distribution reports, applicable discrimination reports and a copy of IRS Form 5500 information returns. Statement files are reviewed for accuracy and approved for processing by the Plan Consulting Team (Control 7.1).

Statement files are processed in batches by Plan and monitored by Mailing Services personnel, who maintain printing and mailing logs to help achieve complete and accurate statement processing (Control 7.2).

BPAS performs trust accounting services for some balance forward plans and certain daily valuation plans. Trust accounting involves the preparation of income statements, balance sheets, IRS Form 5500 information returns, and other reconciliation functions. BPAS processes trust asset report statements quarterly and annually, based on plan year. Statements for Trust accounts are electronically generated after initiating a processing job from the PTM application that pulls historical transaction data from OmniDC for reporting. Quarterly, a member of the Trust department selects a random sample of statements following each production run and confirms the accuracy of each statement by reconciling the balances from the plan summary page back to the OmniDC system (Control 7.3).

## VEBA and Health & Welfare Plans Claims Processing

**Control Objective 8: Controls provide reasonable assurance that system restrictions are configured so that VEBA, HRA, FSA, and HSA claims process through the system completely and accurately.**

Analysts search all web claims that have been uploaded into the Wex Health system. The analyst reviews each submitted attachment by date received to determine if itemized data has been submitted and the transaction has settled in participant account. If further information is required, a letter is sent via email to the participant, requesting further substantiation. Analysts are able to access the web portal and view all uploaded claims, including those that require further substantiation and those that have received additional information from any inquiry.

Each receipt is keyed into participant accounts based on information provided on documentation submitted. Claims cannot be processed until all required fields and required documents have been completed within the system (Control 8.1). All information undergoes a second review as the information is entered into the Wex Health system. The Approval or Denial process is determined at this stage. Once all information is entered, the system detects and reports potential duplicate claims to claims adjudication personnel. (Control 8.3). If duplications are found, a secondary review is required. Receipt will be released for payment if no duplication errors occur.

In the event a claim duplication is detected, the system places the receipt on hold and no payment is authorized. Analyst must then review for possible duplication. If no duplication exists, the claim is manually released for payment (this becomes a manual claim and the transaction is then approved). If the duplication exists, the claim is denied, and a letter is generated notifying the participant of the duplication. A denial letter is also sent via email to the participant, requesting repayment of a denied expense for debit card transactions. Ultimately, the claim is either processed or cleared and the transaction is validated, causing the suspension to be waived in the debit card purse.

Paper claims must be keyed into the application. The system has built-in edit checks so that the information keyed in is complete and accurate (Control 8.2).

## Defined Benefit and Other Postemployment Benefits Valuation

**Control Objective 9: Controls provide reasonable assurance that Defined Benefit (DB) and Other Postemployment Benefit (OPEB) client information is received and input accurately and controls exist to validate the completeness and accuracy of system outputs.**

Actuarial valuation services controls include agreement on scope of service to be provided, collection of data to be relied on, guidelines on doer/checker process, workpapers and computer systems utilized, and signature authority for issuing statement of actuarial opinion (SAO).

BPAS Actuarial & Pension Services requires the completion of a Service Agreement, which outlines the services and responsibilities of each party prior to BPAS Actuarial & Pension Services performing services for the plan sponsor. All new DB and OPEB clients are required to sign a services agreement which outlines the services, fees, and terms and conditions of each engagement. (Control 9.1). The Service Agreement, along with the standard terms of engagement, is considered "evergreen". Absent any changes to the terms of engagement or scope of services, only updates to the Fee Schedule will be issued as they occur.

All collection of data activities is coordinated by the members of the engagement team. Protected information is provided through a Secure File Transfer protocol (BPAS Actuarial & Pension Services or plan sponsor system). Non-protected information is provided via email or regular mail. Some information is provided routinely throughout the year (such as payroll feeds or monthly asset statements). Other information is provided through a formal data request as needed.

Input data and census data is reviewed to determine if all required fields are complete and to verify data validity (Control 9.2).

Information that is received is reconciled with existing database and prior year information by the engagement team member designated as the “doer”. The reconciliation to prior year information and updated database is reviewed by the engagement team member designated as the “checker”. Any discrepancies are resolved. The finalized database is utilized by the valuation systems – Proval and Wystar (OPEVs and DBVAL). These system are designed to value DB and OPEB plans, and parameters are defined by the end user. The doer generates test cases for individual review by the doer and checker. Any discrepancies between test case actual and expected results are resolved. Results for the total plan are generated and reviewed by the checker. The results are imported by the doer into the workpaper template that generates a report. The workpapers and generated report are reviewed by the checker.

Work programs have been developed and are completed by an analyst and checked and reviewed to determine if each required step is performed.

If the checker has signature authority pursuant to the BPAS Actuarial & Pension Services’ signature authority schedule, the report will be final reviewed by a second actuary who cosigns with the checker. All authorized signors must be approved by the BPAS Actuarial & Pension Services Actuarial Practice Committee through the Signature Authority Schedule (Control 9.3). If the checker does not have signature authority, the report will be reviewed by a signing actuary assigned to the engagement and peer reviewed by the second signing actuary.

A review of system outputs, work programs, and the actuarial report is performed and final signoff must be provided by an employee on the Signature Authority Schedule (Control 9.4).

## Defined Benefit Administration

Changes to pension plan participant data are processed throughout the year based on data provided by the plan sponsor.

Benefit election packages are prepared for participants upon request or at required commencement dates.

Participant elections are reviewed and tracked.

To evaluate the completeness of the conversion process for DB Admin clients, the accrued benefit balances reported in the DB Precision application are compared to calculations made external to the application to verify the conversion results. (Control 9.5).

New pension plan distributions are processed based on participant elections. Monthly, distribution totals from Trusts are reviewed to determine if expected changes were processed (Control 9.6).

## Software Development and Maintenance

**Control Objective 10: Controls provide reasonable assurance that new application systems and changes to existing application and supporting systems are documented, tested, and approved.**

### Systems Maintenance

BPAS follows formal system software change management procedures so that production system software changes are implemented in a controlled and secure manner (Control 10.1). The IT Department is responsible for the overall patch management implementation, operations, and procedures. While safeguarding the network is every user's job, IT evaluates if all known and reasonable defenses, patches, hot fixes, service packs, software versions, and firmware versions are in place to reduce network vulnerabilities while keeping the network operating. The Windows patch management system is used for accessing, notification, and scheduling the majority of the networks' patching needs. Additional vendor notifications and web sites are monitored for patch notices.

## **Software Development**

It is the policy of BPAS that all major core processing software applications are acquired from outside vendors/suppliers. Major software applications will not be developed in-house. Software may be developed to provide things such as application interfaces, ad hoc reporting, and workflow engineering. This development is to be kept to a minimum.

## **Application System Changes**

For standard program changes, a Programming Request Form is completed and submitted prior to any modifications/ enhancements being made to system code, configurations or report. IT and Operations Management is responsible for reviewing, testing, and approving change requests (Control 10.2).

For more significant system software upgrades and changes, these changes are coordinated, tested, and approved following a management process.

### OmniDC Upgrades and Configuration Changes

All software upgrades and configuration changes related to the OmniDC system are coordinated by the Senior Vice President (SVP) of Recordkeeping and Trading Services. Program development functions are also managed and supervised by the SVP of Recordkeeping and Trading Services. These projects are initiated through a Programming Request form submitted by a BPAS employee at the request of an internal party or external vendor/customer.

Major requests are reviewed by the management team and then analyzed and classified according to the following criteria:

- Priority
- Business Purpose
- Description
- Detail

Once the project has been appropriately analyzed and classified, the SVP of Recordkeeping and Trading Services provides a final approval to confirm the project for development. At this point, the project is assigned to a BPAS Analyst or Project Manager, who will then be responsible for logging and tracking the project to completion.

## **Operating System Changes**

The IT Department continuously monitors upgrades, releases, and patches that have been made available. This includes network operating systems, individual desktop operating systems and software, electronic mail operating systems, proxy server operating systems, network backup and recovery systems, and the host processing operating system. The changes made within these upgrades are examined in order to determine the urgency of the need to apply the modifications following our Change Management Program.

The Organization utilizes the ManageEngine Desktop Central application to automatically check for Operating System updates on a daily basis. A member of the IT staff checks the management console daily to confirm that all systems are up to date. Any critical issues are reported to the IT Management Team who investigate and address each issue as soon as possible. Once a week, a report is generated, detailing all of the updates.

The ManageEngine Desktop Central management console allows administrators to group servers according to function and priority. One such group is the test group, which houses the Organization's test and development servers. Updates are installed to the test group prior to being installed to production servers. If the patches do not cause any issues for this test group, the patches are applied to the remaining workstation within the week.

All upgrades, releases, and patches are scheduled for implementation during off-peak hours. All installations are performed under the direct supervision of the IT Department.

In the event that a problem occurs that a patch to be installed outside the regularly scheduled times, the IT Department implements the necessary updates and notifies BPAS management.

## Logical Access

**Control Objective 11: Controls provide reasonable assurance that logical access to applications, data, and supporting systems is limited to authorized individuals.**

### Information Security Policy

BPAS realizes that the rapidly changing nature of technology and the critical nature of strategic core processing systems are vital to the success of the Organization. CBSI has implemented a comprehensive Information Security Policy to address all areas of information systems and technology, including sub policies around End-User Computing, Mobile Device and Remote Access, Network Security, Incident Response, Privacy and Vendor Management. (Control 1.1).

The Information Security Policy also addresses information sensitivity and confidentiality and appropriate security measures are in place to safeguard customer and Company information. The Organization's security program is also designed to consider the protection of customer information against any anticipated threats or hazards to the security or integrity of such information, manage the accountability of users with access to sensitive information confirm the availability of information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

### Information Technology Roles and Responsibilities

The Information Technology (IT) Department has the primary responsibility for day-to-day oversight of information systems. Information systems oversight duties of the IT Department include:

- Monitoring operations of all computers and software.
- Troubleshooting systems problems.
- Maintaining current inventories of the software and hardware components.
- Capacity monitoring and planning for all systems.
- Acquiring and deploying systems.
- Disaster recovery.
- Installing new software and upgrading existing software.
- Managing outsourced vendor relationships.
- Cooperating fully with regulatory and auditing agencies.

Information Security oversees all security-related policy matters and functions within the Organization. Technology Services implements the approved security policies and monitoring tools. These roles and responsibilities between the two groups as it relates to security include, but are not limited to, the following functions:

- Assists the Organization in the formulation of security policies and procedures.
- Implement approved security policies and procedures.
- Administers security on critical information processing systems.
- Implements network software tools that monitor user and file access.
- Monitors daily security reports for unauthorized access to networks and application systems.
- Keeps abreast of current technology, security software updates, and security methods through attending seminars and reading periodicals.
- Maintains an awareness of ever-changing security considerations and precautions by monitoring key industry security web sites.



### **Logical Access Administration**

Access to administer applications, servers, and databases is limited to operations staff based on their job responsibilities (Control 11.1). Managers and supervisors authorize the nature and extent of user access privileges for new employees (Control 11.2). Appropriate roles and responsibilities are documented on a Resource Authorization form. The form is sent to the IT staff for access provisioning. Network and application access profiles are created by a Support Technician and initial logon credentials are provided to the new hire. Terminations are communicated to the security administrators. User access privileges are then modified to restrict user access. (Control 11.4). Annually, management completes a user access level review for the BPAS systems to determine if access permissions reflect a user's current job responsibilities. (Control 11.3).

### **Password Controls**

Each strategic system may vary as to the level of password construction supported, as well as the ability to automatically enforce adherence to a standard. When possible within a strategic system, the following minimum password criteria will be used and automatically enforced:

- The primary Windows passwords must be at least fourteen characters in length. For ancillary systems, there is a requirement for at least 8 characters in length, however the recommendation is using the Windows requirements where feasible.
- Passwords must be changed every 90 days. An employee may elect to change their password at any time, but if a password is not changed within 90 days, the system will force a password change.
- All passwords are suppressed from all output.
- Passwords must be "complex" and contain both alpha and numeric characters, at least three alpha numeric mixed with numeric.
- There are no restrictions on repeating characters, outside of Windows complexity rules; however, the password must contain some change.
- A password history of 24 passwords will be maintained.

The above standards are also followed for those systems that can support them but are not capable of automated enforcement. On other systems, the Organization will require users to use a mixture of letters and numbers in the password up to the length of password supported by that particular system (Control 11.5).

### **Security Monitoring**

The anti-virus security, next generation endpoint agents and firewalls are configured to monitor security activities and protect against threats in real time. The status of all servers and workstations is scanned from a control station daily. Alerts are displayed at workstations and at the control station if virus definition files are out of date. System monitoring software is also configured to send email alerts to operations staff to notify them of problems with key services and server resources.

In addition, the Organization has developed and implemented a daily IT Operations Checklist to review and verify security monitoring procedures and infrastructure health on a daily basis. IT and Information Security personnel review the following monitoring logs:

- OpManager Technology Infrastructure Logs
- SolarWinds
- Backup Logs
- SIEM Logs
- Endpoint Security Logs
- SQL Server Logs
- Visual Computer Room Check  
AD Lockout Report

## Security Breaches

Even though the organization has established a number of layered security controls along with policies and procedures, appropriate planning is in place in the event a security event was to occur. If one is detected, Information Security will initiate our Incident Response Plan with some of the key components included below:

- Assemble the Response Team;
- Assess the Situation;
- Involve Executive Management and Third Parties;
- Perform “Triage”;
- Investigate the Breach;
- Determine if the Situation Triggers Consumer Notification;
- Where Required or Deemed Appropriate, Inform Law Enforcement and Applicable Regulatory Entities;
- Take Steps to Reduce Risk and Minimize Losses;
- Notify Third Parties;
- Implement the Communications Plan;
- Document the Event and Conduct a Response Assessment

## Backups

**Control Objective 12: Controls provide reasonable assurance that critical applications and data are backed up to an off-site location.**

BPAS has developed and maintains a formally defined Backup and Retention policy (Control 12.1). All database files for the OmniDC and CensusPro applications are backed up daily using a tape backup system (Control 12.2). Other production data including transaction logs, support files, and secondary SQL databases are also backed daily. Current backup tapes and archived tapes are rotated off-site in accordance with the policy. An off-site storage facility is used to store backup tape medium. (Control 12.4). Daily, a backup log is used to document the success or failure of backup jobs, any necessary corrective action, and the volume of data on the backup tape. (Control 12.3).

In addition to tape backups, BPAS uses two auxiliary backup methodologies to confirm data integrity and availability. OmniDC, as well as other core applications, are replicated in real-time to the BPAS Disaster Recovery site. Validation tests are performed periodically to evaluate if the databases are in sync. In addition, the OmniDC application and its database files are backed up daily to an independent backup server also located in the BPAS Data Center. This production-ready system is maintained to allow for immediate recovery in the event of a catastrophic hardware or software failure.

## System Processing and Performance Monitoring

**Control Objective 13: Controls provide reasonable assurance that system capacity and performance are monitored by IT personnel.**

An IT operations checklist is followed to confirm all daily system capacity, security and performance monitoring tasks are performed by the IT Operations personnel (Control 13.1). An IT operations checklist is followed to confirm all daily system capacity, security and performance monitoring tasks are performed by the IT Operations personnel (Control 13.2).



## Physical Security

**Control Objective 14: Controls provide reasonable assurance that environmental and physical safeguards restrict unauthorized access to the data center and protect against the destruction of computer hardware.**

A majority of the core systems supporting BPAS's operations are located within the BPAS data center in Utica, New York. The Utica data center also hosts the primary LAN equipment for the Organization's benefit administration operations. Remote offices and other facilities connect to the systems in the Utica data center using secure dedicated connections (MPLS IPVPN). Routers are installed at each office to facilitate the WAN between operations centers.

### Access Control Systems

Facility doors are secured with electronic key fob readers and remain locked at all times. The exterior main entrance door is open to visitors between 9 am and 4 pm. The internal door remains locked at all times, and all visitors at this entrance must be allowed in by the receptionist, and subsequently sign a visitor's log before entering the facility. The physical access systems are maintained by a third-party organization.

Physical access to the BPAS Data Center is restricted by an electronic key fob system. Only authorized personnel have physical access to the data center in accordance with the Organization's physical access policy (Control 14.1). Management authorization is required to obtain Data Center key fobs.

### Fire Detection and Suppression Equipment

BPAS has a single, building-wide smoke detection system that features hard-wired alarms and strobe lights throughout the building. This detection system is tied into the facility alarm system and will alert appropriate emergency response personnel in the event of a fire. Fire suppression is provided by an FM-200 chemical suppression system. In addition, two chemical fire extinguishers (Type ABC) are located in the Data Center. On annual basis, the fire and smoke detection equipment, FM-200 chemical fire suppression system, and fire extinguishers are tested by a third party (Control 14.2).

### Emergency Power Equipment

BPAS utilizes a battery and generator uninterruptible power supply (UPS) system to protect computer equipment from variations in electrical current and complete power outages. The system is comprised of two 30KVa Liebert battery units and a diesel generator. The batteries can provide 60 minutes of backup at normal active load, allowing time for the generator to engage. On average, it takes the generator less than a minute for startup and failover.

## Subservice Organization Monitoring Controls

**Control Objective 15: Controls provide reasonable assurance that subservice organizations are identified and performance is evaluated in accordance with the vendor management policy.**

A vendor management program has been established at the corporate level and is adopted throughout the organization. Policies and procedures are in place to govern the vendor management process including but not limited to the acquiring, assessment, and risk exposure of third-party vendors (Control 15.1). Utilizing regulatory guidance along with industry best practices, the policy and procedures that have been created outline the process to select, assess, and monitor third-party relationships. Starting with the planning/due diligence phase, guidance is provided that assists the business owner to select a competent and qualified vendor, while at the same time including criteria to help determine whether the relationship should be included in the vendor management program. For relationships that meet the criteria, the next phase assesses and rates the risk exposure the third party represents to the organization. Utilizing a risk assessment that focuses on strategic, reputation, operational, transaction, credit, and compliance risks, an inherent risk score is established. In addition, the assessment also focuses on mitigating controls, which in combination with the inherent risk score create an overall residual risk for each relationship. The next phase of the process focuses on contract negotiation, which may run in parallel with the initial risk assessment. The guidance provided can assist both the business owner and the Legal department, when applicable,

with contractual provisions that can be considered during the negotiation process. Guidance is also provided that establishes thresholds on when additional review and approval is warranted. Also running in parallel once the risk assessment has been completed, request and review of monitoring documents should take place that is dependent on the level of inherent risk the relationship poses to the organization. The requirements are on a progressive scale, so those identified as a Low risk without the transfer of sensitive data are considerably less than a relationship identified as a High risk. The documentation collected allows the appropriate internal parties to review the controls in place and determine whether additional mitigating controls are warranted.

On an annual basis, similar steps are taken to refresh the risk assessment originally established and to request that similar monitoring documents are collected to determine the risk level and controls in place still adhere to expectations. The exception to the annual review process due to the size of the vendor management program is that those relationships considered to be a Low risk will only have the monitoring documents collected and reviewed every other year; however, they are still risk assessed on an annual basis. The final phase of the process is when the relationship has terminated due to various reasons and guidance is provided to appropriately transfer any sensitive information that may be contained by the third party per agreement in order to bring the relationship to an end.

The vendor management program, including inventory of third parties, is owned and maintained by the CBSI Information Security Department, which works closely with the various business owners of these relationships throughout the organization.

Specifically, for the subservice organization that is noted in this report, on an annual basis, management evaluates the subservice organizations controls through questionnaires and/or through the review of SOC reports (Control 15.2).

## Complementary User Entity Controls

The BPAS Plan Administration and Recordkeeping Service control structure is designed with the assumption that certain controls would be implemented by user entities. This section describes user entity controls identified by BPAS as necessary to achieve the specified control objectives.

The user entity controls described below should not be regarded as a comprehensive list of all controls which should be employed by user entities. Each user entity's internal control over financial reporting should be evaluated in conjunction with BPAS's controls and the complementary user entity controls identified below.

User entities are responsible for the following:

Complementary User Entity Controls	Related Control Objectives
Authorized Plan Representative should be responsible for monitoring the accuracy of changes to user entity accounts.	Control Objectives 2, 3, 4, & 9
Authorized Plan Representatives should determine if all participant enrollments are authorized.	Control Objectives 2, 3, 4, & 9
Timely written notification of changes to the plan, its objectives, participants, and investment managers is communicated to BPAS.	Control Objectives 2, 3, 4, & 9
Timely written notification of changes in the designation of individuals authorized to instruct BPAS regarding activities, on behalf of the user entity, is communicated to BPAS.	Control Objectives 2, 3, 4, & 9
Timely written notification of changes in related parties for purposes of identifying party-in-interest transactions is communicated to BPAS.	Control Objectives 5 & 9
Timely review of reports provided by BPAS of user entity account balances and related activities is performed by the user entity, and written notice of discrepancies is provided to BPAS.	Control Objectives 5 & 9
Physical and logical access to BPAS's systems via terminals at user locations are restricted to authorized individuals.	Control Objectives 11 & 14
Users of the BPAS Sponsor Web and CensusPro should implement controls surrounding User IDs and passwords established for account use. Passwords should be different from the User ID, contain both letters and numbers, be difficult to guess, and be routinely changed.	Control Objectives 11

## Subservice Organizations

This section outlines that certain control objectives specified by BPAS can be achieved only if complementary subservice organization controls assumed in the design of BPAS’s controls are suitably designed and operating effectively, along with the related controls at BPAS. The description of controls in this report includes only the policies, procedures, and controls at BPAS and does not include policies, procedures, and controls at the third-party service provider described below. The examination by the Independent Service Auditors did not extend to policies and procedures at this third-party organization. The primary, relevant third-party service provider used by BPAS is listed below. Please refer to the description content under the header “Subservice Organization Monitoring Controls” for a summary of the activities performed by BPAS to monitor this subservice organization.

Subservice Organization	Services Provided	Controls Expected to be Implemented at the Subservice Organization
Wex Health	Hosting and development of the Wex Health Cloud healthcare accounts administration platform.	<p>Control Objective 10 (Software Development and Maintenance)</p> <ul style="list-style-type: none"> <li>• Application and database changes have approval from IT management prior to migration to production.</li> <li>• Application and database changes have been tested prior to migration to production.</li> <li>• Direct update access to production source and executable libraries, and the ability to migrate changes to production is restricted to authorized individuals using access control and change management systems.</li> </ul> <p>Control Objective 11 (Logical Access)</p> <ul style="list-style-type: none"> <li>• Administrative and/or privileged access to applications, operating systems, databases, and the network level is restricted to authorized individuals.</li> <li>• Local and remote users are subject to password controls when authenticating and accessing systems.</li> <li>• Managers and supervisors authorize the nature and extent of user access privileges.</li> <li>• Termination and transfers of employees and contractors are communicated to the security administrators. User access privileges are then modified to restrict user access accordingly.</li> <li>• Management should complete at a user access level review at least annually.</li> </ul> <p>Control Objective 12 (Backups)</p> <ul style="list-style-type: none"> <li>• Backups are monitored for successful completion according to the defined schedule. Any failures are investigated and corrected.</li> <li>• All system backups are automatically verified for integrity after a backup is performed.</li> <li>• Backups are automatically and electronically replicated to an off-site location.</li> </ul>

Subservice Organization	Services Provided	Controls Expected to be Implemented at the Subservice Organization
		<p>Control Objective 13 (System Processing and Performance Monitoring)</p> <ul style="list-style-type: none"> <li>• Job processing is monitored and reviewed continuously for successful completion by data center staff.</li> </ul> <p>Control Objective 14 (Physical Security)</p> <ul style="list-style-type: none"> <li>• Access to the data center facilities where computer processors, disk and tape storage devices, tape library, communications equipment, and consoles are stored is restricted to authorized individuals.</li> <li>• Access to data center facilities is reviewed at least annually and access rights are modified accordingly.</li> </ul>

# SECTION IV: Independent Service Auditor's Description of Tests of Controls and Results

## Overview of Crowe LLP's Test Procedures

Our examination was restricted to the control activities specified by Benefit Plan Administrative Services, Inc.'s (BPAS or Company or organization or service organization) management in Sections III and IV of this report to address the control objectives that were stated in the description. Our examination did not extend to any other control procedures, including those that may be described in Section III but not listed in Section IV.

The following table clarifies certain terms that may be used within this section to describe the nature of the tests of controls performed:

Type of Testing	Description
Observation	Observed the application, performance or existence of the specified controls as described.
Inspection	Inspected manually or systematically maintained documentation to evidence performance of the specified controls.
Reperformance	Reperformed the specified controls as performed by management to compare our independent results to those of management.

As Crowe conducted inquiry with appropriate BPAS personnel for all controls, inquiry was not listed specifically by each control within Section IV.

In addition, when using information produced by BPAS, we performed procedures as required by AT-C Section 320 to validate whether the information was sufficiently reliable for our purposes by obtaining evidence about the completeness and accuracy of such information, as well as evaluating whether the information produced was sufficiently precise and detailed for our purposes.

## Control Objective 1: Management Oversight and Governance

Control Objective 1: Controls provide reasonable assurance that the overall management and governance structure is established and implemented by the organization.			
Control Number	Description of Controls	Tests of Operating Effectiveness	Results
1.1	CBSI has implemented a comprehensive Information Security Policy to address all areas of information systems and technology, including sub policies around End-User Computing, Mobile Device and Remote Access, Network Security, Incident Response, Privacy and Vendor Management.	Inspected the organization's Technology and Information Security policies and procedures to determine if they outlined the organizations standards as it relates to access to and disclosure of sensitive data.	No exceptions noted.
1.2	Employees are required to acknowledge their agreement to the Company Code of Conduct and to the policies defined within the Employee Handbook upon hire.	Inspected policy acknowledgement documentation for a sample of new employees to determine if new employees are required to acknowledge their agreement to the Company Code of Conduct and to the policies defined within the Employee Handbook.	No exceptions noted.
1.3	Every other week, BPAS management meets and discusses the organization's operations, including risks facing the organization and its information systems.	Inspected meeting minutes for a sample of BPAS management meeting occurrences to determine if BPAS management meets to discuss operations, including risks facing the organization.	No exceptions noted.
1.4	The Human Resources department issues job descriptions to all new hires in conjunction with the hiring process. Job descriptions include a description of the position's roles and responsibilities	Inspected job descriptions for a sample of new employees to determine if a job description existed for positions that were filled during the examination period and that the job description included a description of the position's roles and responsibilities.	No exceptions noted.
1.5	The departments, functional areas, and the reporting lines associated with each are documented in an organization chart.	Inspected organizational charts to determine if these show the separate functional areas and the reporting lines associated with each functional area.	No exceptions noted.



## Control Objective 2: Benefit Administration and Transaction Processing

Control Objective 2: Controls provide reasonable assurance that new plan sponsors, plan participants, and participant loans are authorized and approved and then processed completely and accurately.

Control Number	Description of Controls	Tests of Operating Effectiveness	Results
2.1	All prospective plans are reviewed by the New Account Review Committee prior to being accepted by BPAS and initiation of the implementation process. Accounts are initiated when a plan sponsor requests service and executes the agreements to retain BPAS to provide such services. If a plan sponsor has a direct contractual relationship with BPAS, an OFAC (Office of Foreign Assets Control) scan is performed to verify that the company is not on any of the government watch lists.	Inspected New Account Review Committee meeting minutes and OFAC check documentation for a sample of new plans accepted during the examination period to determine if new plans were approved by the New Account Review Committee and that new plans passed an OFAC check.	No exceptions noted.
2.2	BPAS requires the completion of a Service Agreement that outlines the services to be performed, each party's responsibilities, and administrative fees of each party prior to BPAS performing services for the plan.	<p>Inspected the services agreement for a sample of new plans accepted during the examination period to determine if a signed Service Agreement was on file that covered the services to be performed and each party's responsibilities and this agreement was signed prior to providing services.</p> <p>Inspected system evidence showing the configured administrative fees for a sample of new plans accepted during the examination period to determine if the fees outlined in the Services Agreement matched the fees coded in the OmniDC system.</p>	No exceptions noted.

Control Objective 2: Controls provide reasonable assurance that new plan sponsors, plan participants, and participant loans are authorized and approved and then processed completely and accurately.			
Control Number	Description of Controls	Tests of Operating Effectiveness	Results
2.3	New plan sponsors, financial intermediaries, and BPAS sales associates are required to complete the BPAS Installation Kit to capture the necessary information required to establish the new plan at BPAS.	Inspected the Installation Kit for a sample of new plans accepted during the examination period to determine if the Installation Kit was completed and retained in the plan's records.	No exceptions noted.
2.4	A New Account Checklist is completed by BPAS to evaluate the completeness of the implementation process.	Inspected the new account checklist for a sample of new plans accepted during the examination period to determine if the New Account Checklist was completed and retained in the plan's records.	No exceptions noted.
2.5	New plans are established in the Plan and Task Manager (PTM) application and a Plan Consultant is assigned to administer the Plan Sponsor once all plan information has been obtained.	Inspected documentation from the PTM application for a sample of new plans accepted during the examination period to determine if plans are established in PTM and that a Plan Consultant is assigned.	No exceptions noted.
2.6	The Conversion Team reviews the information provided by the plan sponsor and generates a summary document out of Omni to determine if participant information items such as eligibility, vesting, methods of allocation and other pertinent provisions were completed. A Plan Consultant performs a secondary review.	Inspected review documentation for a sample of new plans accepted during the examination period to determine if an initial review was completed by the Conversion Team and a secondary review was completed by the Plan Consultant to evaluate if all necessary information had been completed.	No exceptions noted.

Control Objective 2: Controls provide reasonable assurance that new plan sponsors, plan participants, and participant loans are authorized and approved and then processed completely and accurately.			
Control Number	Description of Controls	Tests of Operating Effectiveness	Results
2.7	To determine if plan assets are recorded accurately, the BPAS Conversion Team reconciles the plan assets and enters the information into the OmniDC accounting system. A Conversion Specialist, working in conjunction with the Plan Consultant, reviews all plan documents and evaluates if the plan is coded accurately into the system by reviewing the "DECON PACK," which compares the new data coded into the system with the data provided by the plan sponsor	Inspected plan asset review documentation for a sample of new plans accepted during the examination period to determine if plan assets were reviewed by a Conversion Specialist to evaluate if the plan was coded correctly into the system.	No exceptions noted.
2.8	A Conversion Checklist is completed by the Conversion Manager to evaluate the completeness of the conversion process for new plans.	Inspected the Conversion Checklist for a sample of new plans accepted during the examination period to determine if the Conversion Checklist was completed for new plans.	No exceptions noted.
2.9	Qualified employee additions to existing plans are communicated when participant information is received through census data communicated from the plan sponsor. The submitted participant addition is then uploaded into OmniDC during the contribution processing cycle.	Inspected plan addition request documentation and screenshots from plan detail screens in OmniDC for a sample of new participants to determine if participant information was communicated through census data provided by plan sponsors and the submitted participant additions were entered accurately into OmniDC.	No exceptions noted.

Control Objective 2: Controls provide reasonable assurance that new plan sponsors, plan participants, and participant loans are authorized and approved and then processed completely and accurately.			
Control Number	Description of Controls	Tests of Operating Effectiveness	Results
2.10	Plan participants complete a Standard Investment Election Form that is communicated to BPAS for transaction processing. Transactions are then entered by a Processor and independently reviewed by another Processor.	Inspected the Standard Investment Election Form and investment election transaction review documentation for a sample of new investment election transactions to determine if the Standard Investment Election Form was completed by the applicant and an independent review was performed by another Processor.	No exceptions noted.
2.11	Traditional participant loans are requested through the completion of a standard Loan Request Form. All requests are reviewed by a Participant Services Representative or a Distribution Specialist to determine if they were accurately completed and then entered within BPAS systems.	Inspected the loan request form and loan review documentation for a sample of traditional participant loans to determine if a loan request form was completed by the applicant and the traditional participant loan was reviewed for accuracy by a Plan Consultant or Distribution Specialist.	No exceptions noted.
2.12	Participant loans through the MyPlanLoan program are requested and automatically permitted based on plan terms through the BPAS website.	Inspected system screenshots and other related supporting documentation for a sample of MyPlanLoan loans to determine if the participant's plan allowed MyPlanLoan loans and that the requested loan amount agreed to the balance loaned to the participant.	No exceptions noted.

### Control Objective 3: Participant Plan Changes

Control Objective 3: Controls provide reasonable assurance that changes to existing plans and participant records are authorized.			
Control Number	Description of Controls	Tests of Operating Effectiveness	Results
3.1	All plan amendments are signed by the client and maintained for confirmation. Plan documents and amendments are prepared by the Document Services Team	Inspected participant investment request documentation and screenshots from OmniDC for a sample of participant investment election changes to determine if the investment election change request was submitted by the customer and the participant investment election was entered accurately into OmniDC.	No exceptions noted.
3.2	Transactions requested through the BPAS Voice Response Unit (VRU) and the BPAS web site can only be processed if a Participant Identification Number (PIN) is entered into the system.	Inspected system configuration evidence to determine if a unique Participant Identification Number (PIN) is required to initiate transactions via the BPAS VRU system and the BPAS web site.	No exceptions noted.
3.3	Participant terminations are communicated when census data is received from plan sponsors and these participant termination requests are then processed within the OmniDC system.	Inspected participant termination request documentation and screenshots from OmniDC for a sample of terminated participants to determine if a participant termination request was submitted by the customer and the participant's status in the OmniDC application was updated to reflect their termination.	No exceptions noted.
3.4	BPAS requires written authorization from the plan sponsor to terminate or close an account.	Inspected written termination authorization documentation for a sample of plans that were terminated during the examination period to determine if there was written authorization to support plan terminations.	No exceptions noted.

## Control Objective 4: Participant Deferrals and Contributions

Control Objective 4: Controls provide reasonable assurance that participant deferrals are accounted for and contributions to employee benefit plans are processed completely and accurately.			
Control Number	Description of Controls	Tests of Operating Effectiveness	Results
4.1	Census data received electronically is automatically validated by the CensusPro (CPRO) application during the upload process. CensusPro requires the correction of file format errors by the plan sponsor prior to permitting the file to be uploaded for processing.	Inspected system configurations from the CensusPro application to determine if the system has automatic format validation checks that prevent further processing if file format errors exist.	No exceptions noted.
4.2	Daily, CPRO reports are automatically generated that summarize if census data files successfully uploaded to the BPAS web servers.	Inspected CPRO reports for a sample of days to determine if the CPRO application automatically generated reports that summarize if census data files successfully uploaded to the BPAS web servers.	No exceptions noted.
4.3	The OmniDC application prevents contributing participant deferrals and/or employer contributions to funds not authorized for investment by plan sponsors.	Inspected system configurations from the OmniDC application to determine that when participant contributions to funds are not authorized for investment, an error message that generates and prevents further processing.	No exceptions noted.
4.4	Plan eligibility requirements by contribution source are defined within the OmniDC application, which prevents non-qualified employees from contributing until all plan requirements have been achieved to become a valid participant.	Inspected system configurations from the OmniDC application to determine that when a non-qualified employee attempts to contribute before achieving all requirements needed to become a valid participant, an error message that generates and prevents further processing.	No exceptions noted.

**Control Objective 4: Controls provide reasonable assurance that participant deferrals are accounted for and contributions to employee benefit plans are processed completely and accurately.**

<b>Control Number</b>	<b>Description of Controls</b>	<b>Tests of Operating Effectiveness</b>	<b>Results</b>
4.5	A Plan Administration Checklist is completed by the Plan Consultant to document the year-end employer allocations and required discrimination testing performed by BPAS in accordance with plan terms.	Inspected the overall Plan Administration Checklist tracking documentation and the Plan Administration Checklist for a sample of plans to determine if checklists were completed to evaluate if year-end allocations and discrimination testing were completed.	No exceptions noted.
4.6	Daily, transactions entered into the OmniDC system are compared to the Net Trade Recap Report to assess the accuracy of the contribution information that was entered and processed.	Inspected the Net Trade Recap Report and other related supporting documentation for a sample of days to determine if management completed a review to assess the accuracy of the contribution information that was entered and processed.	No exceptions noted.



## Control Objective 5: Trade Processing

Control Objective 5: Controls provide reasonable assurance that trades are recorded completely and accurately.			
Control Number	Description of Controls	Tests of Operating Effectiveness	Results
5.1	Contribution and distribution transactions to be traded are flagged with a system status change from "EDIT" to "PROD" in the OmniDC application. Once these distribution and contribution transactions are completed, the system status is updated to "SUCCESSFUL".	Inspected system configurations to determine if transactions to be traded have their system status changed from "EDIT" to "PROD" in the OmniDC application and the status of transactions gets updated to "SUCCESSFUL" once they are successfully processed.	No exceptions noted.
5.2	Transactions that require prices that are not available are placed in a system status of "HOLD" and will not be processed that evening.	Inspected system configurations to determine if transactions that require an unavailable price are placed in a system status of "HOLD" in the OmniDC application.	No exceptions noted.
5.3	Daily, the Trading Checklist is completed during the preparation of the trade order files. The checklist includes a requirement for reviewing and reconciling the total trades and dollar totals from the Order file.	Inspected the Trading Checklist for a sample of days to determine if the checklist was completed by management.	No exceptions noted.

## Control Objective 6: Participant Disbursements and Payments

Control Objective 6: Controls provide reasonable assurance that disbursements and payments to participants are authorized and remitted completely and accurately.			
Control Number	Description of Controls	Tests of Operating Effectiveness	Results
6.1	Participant Service Representatives or Distribution Specialists review disbursement requests to evaluate if all required paperwork and authorizations were completed.	Inspected disbursement request review documentation for a sample of participant disbursements to determine if disbursements are reviewed by a Customer Service Representative or a Distribution Specialist to evaluate if all required paperwork and authorizations were completed.	No exceptions noted.
6.2	Terminating participants that are requesting a final distribution must complete the required forms and return them to BPAS prior to disbursement.	Inspected terminating participant distribution forms for a sample of disbursements for terminating participants to determine if all required termination forms were completed.	No exceptions noted.
6.3	Daily, a Summary Trade Order report illustrating plan investment transactions is prepared by a BPAS Trust Operations employee to verify the total dollar amount and accuracy of the disbursements. The report is then reviewed by an independent Trust Operations employee prior to faxing the request to the Wire Desk for execution.	Inspected the Summary Trade Order report and other supporting review documentation for a sample of days to determine if the Summary Trade Order report was prepared and then reviewed by an independent Trust Operations employee.	No exceptions noted.
6.4	Daily, BPAS completes a Wire Procedure Checklist to verify the daily trading activity and authorization of wire transfers of funds. The Wire Procedure Checklist is independently reviewed for confirmation.	Inspected the Wire Procedure Checklist and other supporting review documentation for a sample of days to determine if the Wire Procedure Checklist was prepared and then reviewed by an independent employee.	No exceptions noted.

## Control Objective 7: Customer Statements

Control Objective 7: Controls provide reasonable assurance that statements provided to participants and plan administrators are complete and accurate.			
Control Number	Description of Controls	Tests of Operating Effectiveness	Results
7.1	Statement files are reviewed for accuracy and approved for processing by the Plan Consulting Team.	Inspected the statement file review documentation for a sample of plans to determine if the statement files were reviewed by the Plan Consulting team.	No exceptions noted.
7.2	Statement files are processed in batches by Plan and monitored by Mailing Services personnel using printing and mailing logs.	Inspected print and mail logs for a sample of plans to determine if printing and mailing logs were completed to monitor statement file processing.	No exceptions noted.
7.3	Quarterly, a member of the Trust department selects a random sample of statements following each production run and confirms the accuracy of each statement by reconciling the balances from the plan summary page back to the OmniDC system.	Inspected statement reconciliation and review documentation for a sample of quarters to determine if the Trust department reconciled and reviewed a random sample of statements following the production run.	No exceptions noted.

## Control Objective 8: VEBA, HRA, FSA, and HSA Claims Processing

Control Objective 8: Controls provide reasonable assurance that system restrictions are configured so that VEBA, HRA, FSA, and HSA claims process through the system completely and accurately.

Control Number	Description of Controls	Tests of Operating Effectiveness	Results
8.1	Claims cannot be processed until all required fields and required documents have been completed within the system.	Inspected system configurations to determine if the system prevents claims from being processed until all required fields and required documents have been completed within the system.	No exceptions noted
8.2	Paper claims must be keyed into the application. The system has built-in edit checks so that the information keyed in is complete and accurate.	Inspected system configurations to determine if the system has built-in edit checks so that the information keyed in is complete and accurate.	No exceptions noted
8.3	The system detects and reports potential duplicate claims to claims adjudication personnel.	Inspected system configurations to determine if the system to determine if duplicate claims were detected.	No exceptions noted

## Control Objective 9: Defined Benefit and Other Postemployment Benefits Administration

Control Objective 9: Controls provide reasonable assurance that Defined Benefit (DB) and Other Postemployment Benefit (OPEB) client information is received and input accurately and controls exist to validate the completeness and accuracy of system outputs.			
Control Number	Description of Controls	Tests of Operating Effectiveness	Results
9.1	All new DB and OPEB clients are required to sign a services agreement which outlines the services, fees, and terms and conditions of each engagement.	Inspected the services agreement for a sample of new DB and OPEB clients to determine if a signed services agreement was on file that covered the services, fees, and the terms and conditions of the engagement and this agreement was signed prior to providing services.	No exceptions noted.
9.2	Input data and census data is reviewed to determine if all required fields are complete and to verify data validity.	Inspected input review documentation for a sample of DB and OPEB clients to determine if the data and census input was reviewed prior to processing.	No exceptions noted.
9.3	Annually, all authorized signors must be approved by the BPAS Actuarial & Pension Services Actuarial Practice Committee through the Signature Authority Schedule.	Inspected the Signature Authority Chart to determine if the BPAS Actuarial & Pension Services Actuarial Practice Committee approves and maintains a schedule showing who is authorized to issue Statements of Actuarial Opinion on behalf of BPAS Actuarial & Pension Services.	No exceptions noted.
9.4	A review of system outputs, work programs, and the actuarial report is performed and final signoff must be provided by an employee on the Signature Authority Schedule.	Inspected system output review documentation for a sample of DB and OPEB clients to determine if a review of system outputs, work programs, and the actuarial report was performed and final signoff was provided by an employee on the Signature Authority Schedule.	No exceptions noted.
9.5	To evaluate the completeness of the conversion process for DB Admin clients, the accrued benefit balances reported in the DB Precision application are compared to calculations made external to the application to verify the conversion results.	Inspected the review documentation for a sample of converted DB clients to determine if the comparison was completed and documented by management.	No exceptions noted.

Control Objective 9: Controls provide reasonable assurance that Defined Benefit (DB) and Other Postemployment Benefit (OPEB) client information is received and input accurately and controls exist to validate the completeness and accuracy of system outputs.

Control Number	Description of Controls	Tests of Operating Effectiveness	Results
9.6	Monthly, distribution totals from Trusts are reviewed to determine if expected changes were processed.	Inspected Trust distribution total review documentation for a sample of months to determine if a review was performed by management to evaluate if expected changes were processed.	No exceptions noted.

## Control Objective 10: Software Development and Maintenance

Control Objective 10: Controls provide reasonable assurance that new application systems and changes to existing application and supporting systems are documented, tested, and approved.			
Control Number	Description of Controls	Tests of Operating Effectiveness	Results
10.1	BPAS follows formal system software change management procedures so that production system software changes are implemented in a controlled and secure manner.	Inspected the BPAS change management procedures to determine if they outlined the organizations change control standards.	No exceptions noted.
10.2	For standard program changes, a Programming Request Form is completed and submitted prior to any modifications/ enhancements being made to system code, configurations or report. IT and Operations Management is responsible for reviewing, testing, and approving change requests.	Inspected change control documentation for a sample of application, operating system, and infrastructure system changes to determine if a supporting Programming Request Form was completed for each change and that changes were reviewed, tested, and approved by IT and Operations Management.	No exceptions noted.



## Control Objective 11: Logical Access

Control Objective 11: Controls provide reasonable assurance that logical access to applications, data, and supporting systems is limited to authorized individuals.			
Control Number	Description of Controls	Tests of Operating Effectiveness	Results
11.1	Access to administer applications, servers and databases is limited to IT operations personnel based on their job responsibilities.	Inspected the administrator listings for in-scope applications, servers, and databases to determine if administrative level access was limited to IT operations personnel.	No exceptions noted.
11.2	Managers and supervisors authorize the nature and extent of user access privileges for new employees.	Inspected user access provisioning documentation for a sample of new employees to determine if a manager or supervisor authorized the nature and extent of user access privileges.	No exceptions noted.
11.3	Annually, management completes a user access level review for the BPAS systems to determine if access permissions reflect a user's current job responsibilities.	Inspected the results from the annual user access level reviews to determine if users and access levels were evaluated and any requested changes were reflected on the system.	No exceptions noted.
11.4	Termination tickets are utilized by the organization to track the access removal tasks that must be completed to restrict the access of terminated employees. Terminations are communicated to the security administrators. User access privileges are then modified to restrict user access.	Inspected the termination ticket and user access removal documentation for a sample of terminated employees to determine if a termination ticket was entered to track the completion of access removal tasks and access was removed from all applicable systems.	No exceptions noted.

Control Objective 11: Controls provide reasonable assurance that logical access to applications, data, and supporting systems is limited to authorized individuals.

Control Number	Description of Controls	Tests of Operating Effectiveness	Results
11.5	Password standards are implemented to control network authentication and application system access. Where the application or system permits, password standards implemented include the following: <ul style="list-style-type: none"> <li>•Password minimum character length</li> <li>•Forced password changes</li> <li>•Account lock out after a minimum number of invalid access attempts</li> <li>•Password history</li> <li>•Password complexity</li> </ul>	Inspected the password parameters for in-scope applications to determine if passwords were configured consistent with published standards.	No exceptions noted.

## Control Objective 12: Backups

Control Objective 12: Controls provide reasonable assurance that critical applications and data are backed up to an off-site location.			
Control Number	Description of Controls	Tests of Operating Effectiveness	Results
12.1	BPAS has developed and maintains a formally defined Backup and Retention policy.	Inspected the BPAS Backup and Retention policy to determine if they outlined the organizations data backup standards.	No exceptions noted.
12.2	Database files are backed up daily using a tape backup system.	Inspected backup configuration evidence to documentation to determine if server files and databases are configured to be backed up nightly.	No exceptions noted.
12.3	Daily, a backup log is used to document the success or failure of backup jobs, any necessary corrective action, and the volume of data on the backup tape.	Inspected the backup log for a sample of days to determine if the backup log was completed each day, noting any corrective action for job failures.	No exceptions noted.
12.4	An off-site storage facility is used to store backup tape medium.	Inspected the tape rotation log to determine if it was maintained by the IT Department and that it recorded the transfer of backup tape media to the off-site facility.	No exceptions noted.

## Control Objective 13: System Processing and Performance Monitoring

Control Objective 13: Controls provide reasonable assurance that system capacity and performance are monitored by IT personnel.			
Control Number	Description of Controls	Tests of Operating Effectiveness	Results
13.1	An IT operations checklist is followed to confirm all daily system capacity, security and performance monitoring tasks are performed by the IT Operations personnel.	Inspected the IT operations checklist for a sample of days to determine if the operations checklist was completed by IT Operations personnel.	No exceptions noted.
13.2	Monitoring software tools are used by IT Operations personnel to monitor the availability, security, and performance of the BPAS network, server resources and system software.	Inspected the system configurations of software monitoring tools and reviewed system reports used by the IT Operations staff to determine if monitoring tools are in place.	No exceptions noted.

## Control Objective 14: Physical Security

Control Objective 14: Controls provide reasonable assurance that environmental and physical safeguards restrict unauthorized access to the data center and protect against the destruction of computer hardware.

Control Number	Description of Controls	Tests of Operating Effectiveness	Results
14.1	Access to the data center is limited to authorized individuals.	Inspected a report of individuals with access to the organizations data center to determine if access is restricted to authorized IT personnel.	No exceptions noted.
14.2	Annually, the fire and smoke detection equipment, FM-200 chemical fire suppression system, and fire extinguishers are tested by a third party.	Inspected system testing documentation to determine if the smoke alarm, FM-200, and fire extinguishers were inspected on at least an annual basis.	No exceptions noted.

## Control Objective 15: Subservice Organization Monitoring

Control Objective 15: Controls provide reasonable assurance that subservice organizations are identified and performance is evaluated in accordance with the vendor management policy.			
Control Number	Description of Controls	Tests of Operating Effectiveness	Results
15.1	Policies and procedures are in place to govern the vendor management process including but not limited to the acquiring, assessment, and risk exposure of third-party vendors.	Inspected the BPAS Vendor Management Policy to determine if they outlined the organizations vendor management standards.	No exceptions noted.
15.2	Annually, management evaluates subservice organizations controls through questionnaires and/or through the review of SOC reports.	Inspected subservice organization control monitoring documentation for the one in scope subservice organization to determine if management reviewed questionnaires and/or SOC reports to evaluate the internal controls that are in place at the subservice organization.	No exceptions noted.

SECTION V: Other Information Provided by Benefit Plan  
Administrative Services, Inc. (Unaudited)



## Disaster Recovery and Business Continuity Planning

Benefit Plans Administrative Services, Inc.'s (BPAS or Organization) recognizes the need for resumption of services in the event of a disaster or serious interruption. Backups of the Organization's information systems and benefit administration records are performed on an ongoing basis. Backup systems and procedures include redundancy to provide immediate recovery. Data backup tapes are taken to an off-site storage facility daily and are periodically restored to a test environment to verify tape and process operation. Data from BPAS's core application systems and databases are also backed up to a secondary system locally and are replicated real-time to the Organization's Disaster Recovery site. The BPAS operations facility is supported by an emergency generator. In addition, critical hardware (e.g., servers and environmental systems) within the BPAS data center are connected to an individual uninterruptible power supply (UPS) systems.

## Privacy Policies

BPAS maintains policies regarding the privacy of personal information. Privacy policies adequately address security measures to safeguard the privacy of personal information whether in electronic, paper, or other forms. Security measures are consistent with sensitivity of the personal information. The Organization's privacy notice posted on the BPAS website describes the general types of security measures used to protect the participant's personal information and identifies the purposes for which personal information is collected, used, retained, and disclosed. BPAS describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information. BPAS collects personal information only for the purposes identified in the notice. The use of personal information is limited to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. BPAS retains personal information for only as long as necessary to fulfill the stated purposes. Access to personal information is restricted. BPAS monitors compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes.

## Regulations and Compliance

BPAS is subject to various regulations and compliance requirements. As part of its overall compliance program, BPAS maintains additional policies and procedures to govern its operations and undergoes regular audits to assure adherence to these requirements. The following list illustrates the audits and reviews that are performed to assure compliance:

1. Trust Related Audits
  - a. Regulation 9 and compliance review
  - b. Compliance audit
  - c. Texas Department of Banking
  - d. Composite Collective Investment Funds (CIF)
2. Broker-Dealer Audits
  - a. Financial Industry Regulatory Authority (FINRA)
  - b. Hand Securities Inc. audit
3. Financial / Operational Audit
  - a. Sarbanes-Oxley Act
  - b. Community Bank System Inc. (CBSI) – internal audit
  - c. Annual financial statement audit
  - d. Hand Benefits & Trust Company audit
  - e. Settling Bank – internal audit and Office of the Comptroller of the Currency (OCC) audit
  - f. Information Technology audit

- 
4. Other Regulatory Compliance Requirements
    - a. Gramm Leach Bliley Act
    - b. Patriot Act
    - c. Bank Secrecy Act
    - d. Anti-Money Laundering